BlackBerry Enterprise Service 10

BlackBerry Device Service Solution

Version: 10.1

Security Technical Overview

BlackBerry

Published: 2013-05-14
SWD-20130514151546118

Contents

1 About BlackBerry Device Service solution security 7
BlackBerry Device Service solution security 7
Device security features 8
Hardware root of trust for BlackBerry devices 9
Architecture: BlackBerry Device Service 9
2 How the BlackBerry Device Service and the BlackBerry Infrastructure authenticate with each other 12
What happens when the BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection 12
Data flow: Authenticating the BlackBerry Device Service with the BlackBerry Infrastructure 13
How the BlackBerry Device Service protects a TCP/IP connection to the BlackBerry Infrastructure 14
3 How devices connect to the BlackBerry Device Service 15
Types of encryption that devices use when they connect to your organization's resources 16
Work Wi-Fi connection 17
VPN connection 17
BlackBerry Infrastructure connection 18
Securing the communication between devices and your organization's network 19
Using Kerberos to provide single sign-on from BlackBerry 10 devices 20
Protecting connections from a device to content servers and application servers 20
How the BlackBerry Device Service manages email messages 21
How devices can connect to the BlackBerry Infrastructure 21
Data flow: Opening a TLS connection between the BlackBerry Infrastructure and a device 22
Encrypting data that the BlackBerry Device Service and devices send to each other over the BlackBerry Infrastructure 22
Device transport keys 22
Message keys 23
Using a VPN with a device 25
Protecting a connection between a device and a work Wi-Fi network 25
How a device and the BlackBerry Device Service protect sensitive Wi-Fi information 26
Layer 2 security methods that a device supports 26
EAP authentication methods that devices support 27
4 Activating devices 30
Activating a device over a wireless connection 30
Data flow: Activating a device over a work Wi-Fi connection or a VPN connection 31
Data flow: Activating a device over a connection to the BlackBerry Infrastructure 33
Activating a device using the BlackBerry Web Desktop Manager 35
Data flow: Activating a device using the BlackBerry Web Desktop Manager 36

5 Managing certificates on devices 38
Certificates that the BlackBerry Device Service and a device use to authenticate with each other 38
Using SCEP to enroll client certificates to a device 39
Managing certificates that a device enrolls using SCEP 39
Data flow: Enrolling a client certificate to a device using SCEP 40
Sending CA certificates to devices 41
6 Using IT policies to manage BlackBerry Device Service security 43
Preconfigured IT policy 43
Resolving IT policy conflicts 44
7 Using BlackBerry Balance to secure BlackBerry 10 devices in your organization's environment for work use and personal use 45
Securing work and personal data and apps on devices 46
How devices classify work and personal data and apps 47
How the BlackBerry Device Service and devices protect work and personal data and apps 49
How the BlackBerry Device Service and devices manage work and personal data and apps 52
Controlling how work and personal apps connect to your organization's network 57
Preventing personal apps on devices from using your organization's networks to connect to the Internet 61
Preventing the BBM Video feature on devices from using your organization's networks 62
8 Using BlackBerry Balance to secure BlackBerry PlayBook tablets in your organization's environment for work use 63
How BlackBerry PlayBook tablets distinguish between work data and personal data 63
How BlackBerry PlayBook tablets protect work data 64
Controlling when BlackBerry PlayBook tablets delete all data in the work space 66
How a BlackBerry PlayBook tablet protects personal data 67
What happens when a user updates or creates files on a BlackBerry PlayBook tablet 68
How a BlackBerry PlayBook tablet controls whether an app is a work or personal app 68
Determining which apps are work or personal apps 69
Comparison of work and personal apps 70
Access rights for work and personal data that the BlackBerry PlayBook OS grants to apps 70
How a BlackBerry PlayBook tablet is designed to prevent BlackBerry Runtime for Android apps from accessing work data or apps 71
Controlling the network connections that work and personal apps on BlackBerry PlayBook tablets can access 71
Using the browser to connect a BlackBerry PlayBook tablet to web servers that support NTLM 71
How work apps are installed on a BlackBerry PlayBook tablet 72
When a BlackBerry PlayBook tablet prevents a user from accessing work data or apps 72
9 Securing work space only devices 73
Securing data 73
Classifying data 74
Protecting data 74
Managing data 75

Controlling app connections ... 80
10 Managing app availability on devices ... 83
Preventing users from installing apps using development tools ... 84
Signing apps ... 84
Protecting a device from malicious apps ... 84
11 Extending messaging security on BlackBerry 10 devices ... 85
Extending messaging security on BlackBerry 10 devices using S/MIME protection ... 86
S/MIME certificates and S/MIME private keys on BlackBerry 10 devices ... 89
S/MIME encryption algorithms that BlackBerry 10 devices use ... 90
Data flow: Sending an email message from a BlackBerry 10 device using S/MIME encryption ... 90
Using S/MIME with a smart card ... 91
12 Protecting data ... 92
Passwords ... 92
Device passwords ... 92
Password changes ... 93
Security timeout ... 98
Data wipe ... 99
Full device wipe ... 99
Work space only wipe ... 101
Back up and restore ... 101
Backup protection ... 102
Restore protection ... 102
Encryption ... 103
Work data ... 103
Personal data ... 103
Media cards ... 103
Home screen message ... 104
BlackBerry Smart Card Reader ... 104
Opening a secure connection to the BlackBerry Smart Card Reader ... 104
Unbinding the current smart card from a device ... 105
Authenticating a user using a smart card ... 106
13 The BlackBerry 10 OS ... 107
The BlackBerry 10 device file system ... 107
How the BlackBerry 10 OS uses sandboxing to protect app data ... 108
How the BlackBerry 10 OS manages the resources on a device ... 108
How the BlackBerry 10 device manages permissions for apps ... 109
How the BlackBerry 10 device verifies the software that it runs ... 109
How the BlackBerry 10 device verifies the boot ROM code ... 109
How the BlackBerry 10 device verifies the BlackBerry 10 OS and its file system ... 109
How the BlackBerry 10 device verifies apps and software upgrades ... 110

How the BlackBerry 10 device prevents the exploitation of memory corruption 110
14 The BlackBerry PlayBook OS 112
The BlackBerry PlayBook tablet file system 112
How the BlackBerry PlayBook OS uses sandboxing to protect app data 113
How the BlackBerry PlayBook OS manages the resources on a tablet 113
How the BlackBerry PlayBook tablet manages permissions for apps 114
How the BlackBerry PlayBook tablet verifies the software that it runs 114
How the BlackBerry PlayBook tablet verifies the boot ROM code 114
How the BlackBerry PlayBook tablet verifies the BlackBerry PlayBook OS and its file system 114
How the BlackBerry PlayBook tablet verifies apps and software upgrades 115
How the BlackBerry PlayBook tablet prevents the exploitation of memory corruption 115
15 Protecting the data that the BlackBerry Device Service stores in your organization's environment 117
Data that the BlackBerry Configuration Database stores 117
Best practice: Protecting the data that the BlackBerry Configuration Database stores 118
16 Cryptographic algorithms, codes, protocols, and libraries that devices support 120
Symmetric encryption algorithms 120
Asymmetric encryption algorithms 121
Hash algorithms 121
Message authentication codes 122
Signature algorithms 122
Key agreement algorithms 123
Cryptographic protocols 123
Internet security protocols 123
VPN security protocols 123
Wi-Fi security protocols 123
Cipher suites that a device supports for opening SSL/TLS connections 124
Cryptographic Libraries 126
VPN cryptographic support 126
Wi-Fi cryptographic support 126
17 Product documentation 128
18 Glossary 131
19 Legal notice 136

About BlackBerry Device Service solution security

1

BlackBerry Device Service solution security

The BlackBerry Device Service solution consists of various components and features that extend your organization's communication methods to BlackBerry devices. The BlackBerry Device Service solution protects data that is in transit at all points between a device and the BlackBerry Device Service.

To protect data that is in transit over Wi-Fi and mobile networks, the BlackBerry Device Service and the device use symmetric key cryptography to encrypt the data sent between them. The BlackBerry Device Service solution is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Device Service solution uses confidentiality, integrity, and authenticity to help protect your organization from data loss or alteration and to ensure that you can have confidence in the security of BlackBerry products.

Principles	Description
Confidentiality	The BlackBerry Device Service solution uses symmetric key cryptography to make sure that only intended recipients can view the contents of email messages.
Integrity	The BlackBerry Device Service solution uses symmetric key cryptography to protect every email message that the device sends and to prevent third parties from decrypting or altering the message data. Only the BlackBerry Device Service and the device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The BlackBerry Device Service or the device rejects a message automatically if it is not encrypted with keys that they recognize as valid.
Authenticity	Before the BlackBerry Device Service sends data to the device, the device authenticates with the BlackBerry Device Service to prove that the device knows the device transport key that is used to encrypt data. The BlackBerry Device Service solution prevents counterfeit devices from impersonating authentic devices by authenticating each device that attempts to register with the BlackBerry Infrastructure.

Device security features

Feature	Description
Protection of data between the BlackBerry Device Service and a device	The BlackBerry Device Service protects data that is in transit between the BlackBerry Device Service and a device. The BlackBerry Device Service and a device can communicate using both transport layer encryption (using AES-256) and TLS.
Protection of work data on a device	• The device protects work data using XTS-AES-256 encryption. • BlackBerry Balance devices isolate the work file system and the personal file system. • BlackBerry Balance devices isolate the work apps and the personal apps.
Protection of personal data on a BlackBerry Balance device	You can use an IT policy rule to require that a BlackBerry Balance device encrypt the data stored in the personal file system. The device then protects the personal data using XTS-AES-256 encryption.
Control of device access to your organization's network	The BlackBerry Device Service allows you to send work Wi-Fi profiles and work VPN profiles to a device so that the device can connect to your organization's network.
Control of the behavior of a device	To control the behavior of a device, you can: • Send IT administration commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values. • Send an IT policy to a device to change security settings. You can use the IT policy to enforce the device password on a BlackBerry Balance device.
Protection of device user information	The device allows a user to delete all user information and application data from the device memory.
Protection of the BlackBerry 10 OS and the BlackBerry PlayBook OS	• When a device starts, it completes integrity tests to detect damage to the kernel. • The BlackBerry 10 OS and PlayBook OS can restart a process that stops responding without negatively affecting other processes. • The BlackBerry 10 OS and PlayBook OS validate requests that apps make for resources on the device.

Feature	Description
Protection of application data using sandboxing	The BlackBerry 10 OS and PlayBook OS use sandboxing to separate and restrict the capabilities and permissions of apps that run on the device. Each application process runs in its own sandbox. The BlackBerry 10 OS and PlayBook OS evaluate the requests that an app's processes make for memory outside of its sandbox.
Protection of resources	The BlackBerry 10 OS and PlayBook OS use adaptive partitioning to allocate resources that are not used by apps during typical operating conditions and to make sure that resources are available to apps during times of peak operating conditions.
Management of permissions to access capabilities	The BlackBerry 10 OS and PlayBook OS evaluate every request that an app makes to access a capability on the device.
Verification of the boot ROM code	The device verifies that the boot ROM code is permitted to run on the device.

Hardware root of trust for BlackBerry devices

Research In Motion ensures the integrity of BlackBerry device hardware and makes sure that counterfeit devices cannot connect to the BlackBerry Infrastructure and use BlackBerry services.

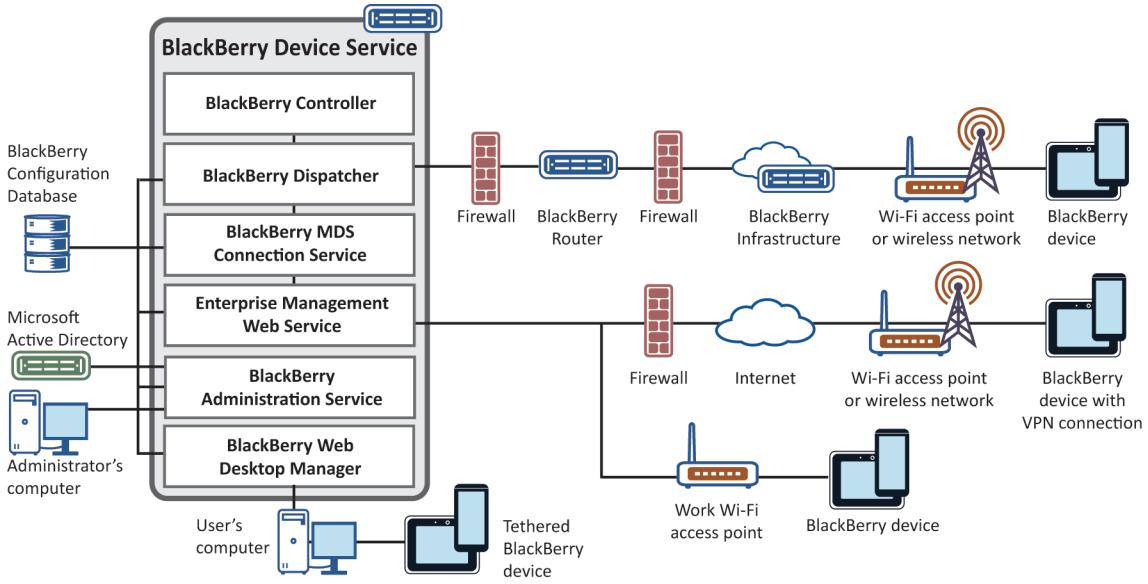
From the beginning of the product lifecycle, RIM integrates security into every major component of the product design of devices so that it is very difficult to remove or bypass this security. RIM has enhanced its end-to-end manufacturing model to securely connect the supply chain, RIM manufacturing partners, the BlackBerry Infrastructure, and devices, which allows RIM to build trusted devices anywhere in the world.

The RIM manufacturing security model prevents counterfeit devices from impersonating authentic devices and makes sure that only genuine BlackBerry devices can connect to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses device authentication to cryptographically prove the identity of the device that attempts to register with it. The device uses its hardware-based ECC 521-bit key pair to verify the integrity of itself and the boot ROM. After the boot ROM is verified, the device verifies the software stack. After the verification process is complete and the device is determined to be authentic, the device tries to register with the BlackBerry Infrastructure. Only devices that are manufactured by RIM and complete the self-verification process can register with the BlackBerry Infrastructure.

Architecture: BlackBerry Device Service

The BlackBerry Device Service consists of various components that are designed to help you perform the following actions:

- Install and manage your organization's applications on devices
- Protect your organization's data and applications on devices



Component	Description
BlackBerry Administration Service	You can use the BlackBerry Administration Service to manage the BlackBerry Device Service and the user accounts and devices that are associated with it. You can manage user accounts and assign groups, administrative roles, software configurations, email profiles, and IT policies to user accounts. You can update user information in Microsoft Active Directory and synchronize that user information manually with the BlackBerry Administration Service. For example, if a user changes their name, you can immediately update their name in both Microsoft Active Directory and the BlackBerry Administration Service. The BlackBerry Administration Service connects to the BlackBerry Configuration Database and to Microsoft Active Directory.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains user account information and configuration information (such as connection details) that the BlackBerry Device Service components use.
BlackBerry Controller	The BlackBerry Controller monitors the BlackBerry Device Service components and restarts them if they stop responding.

Component	Description
BlackBerry Infrastructure	The BlackBerry Infrastructure validates SRP information and controls the IPPP traffic that travels outside your organization's firewall to and from BlackBerry devices.
BlackBerry Dispatcher	The BlackBerry Dispatcher maintains an SRP connection with the BlackBerry Infrastructure over the Internet. The BlackBerry Dispatcher is responsible for compressing and encrypting and for decrypting and decompressing data that travels over the Internet to and from the devices.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between the Enterprise Management Agent on the devices and the Enterprise Management Web Service in the BlackBerry Device Service. The connection is used when the device is not connected to your organization's Wi-Fi network or VPN.
BlackBerry Router	The BlackBerry Router connects to the BlackBerry Infrastructure which sends data to mobile networks or the Internet.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager is a web application that permits users to activate and manage devices.
Enterprise Management Web Service	The Enterprise Management Web Service is a set of web services that communicates commands, configuration information, IT policies, VPN profiles, Wi-Fi profiles, and email profiles between the BlackBerry Administration Service and the Enterprise Management Agent on the devices.
Microsoft Active Directory	The BlackBerry Administration Service obtains user account information from the Microsoft Active Directory that is required to create user accounts in the BlackBerry Device Service.
Work Wi-Fi network	After a device is activated on the BlackBerry Device Service, communication between the BlackBerry Device Service and the device can occur over your organization's Wi-Fi network when the device is within a wireless coverage area and enabled for access according to your organization's network security policies.
External Wi-Fi access point	Depending on your organization's network configuration, communication can occur between the BlackBerry Device Service and devices that are located outside the firewall and connected to the Internet over a Wi-Fi connection.
Firewall	The BlackBerry Device Service requires an outbound-initiated, bidirectional connection through port 3101 on the firewall and over the Internet to the BlackBerry Infrastructure to transport data to and from the devices.
Internet	The Internet transports data between the BlackBerry Infrastructure and the BlackBerry Device Service. Depending on your organization's network configuration, the devices may also communicate with the BlackBerry Device Service using a VPN connection over the Internet.

2 How the BlackBerry Device Service and the BlackBerry Infrastructure authenticate with each other

The BlackBerry Infrastructure and BlackBerry Device Service must authenticate with each other before they can transfer data. The BlackBerry Device Service uses SRP to authenticate with and connect to the BlackBerry Infrastructure.

SRP is a point-to-point protocol that runs over TCP/IP. The BlackBerry Device Service uses SRP to contact the BlackBerry Infrastructure and open a connection. When the BlackBerry Device Service and BlackBerry Infrastructure open a connection, they can perform the following actions:

1. Authenticate with each other
2. Exchange configuration information
3. Send and receive data

The BlackBerry Device Service and BlackBerry Infrastructure use the SRP authentication key when they authenticate with each other. The SRP authentication key is a 20-byte encryption key that the BlackBerry Device Service and BlackBerry Infrastructure share.

What happens when the BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection

After the BlackBerry Device Service and the BlackBerry Infrastructure open an initial connection over the Internet, the BlackBerry Device Service sends a basic information packet to the BlackBerry Infrastructure immediately. A basic information packet includes the BlackBerry Device Service version information, SRP identifiers, and other information that is required to open an SRP connection. Both the BlackBerry Device Service and BlackBerry Infrastructure can recognize the basic information packet. The BlackBerry Device Service and BlackBerry Infrastructure can use the basic information packet to configure the parameters of the SRP implementation.

Data flow: Authenticating the BlackBerry Device Service with the BlackBerry Infrastructure

1. The BlackBerry Device Service sends a data packet that contains its unique SRP identifier to the BlackBerry Infrastructure to claim the SRP identifier.
2. The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Device Service.
3. The BlackBerry Device Service sends a challenge string to the BlackBerry Infrastructure.
4. The BlackBerry Infrastructure hashes the challenge string it received from the BlackBerry Device Service with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to the BlackBerry Device Service as a challenge response.
5. The BlackBerry Device Service hashes the challenge string it received from the BlackBerry Infrastructure with the SRP authentication key, and sends the result as a challenge response to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure performs one of the following actions:

   - Accepts the challenge response and sends a confirmation to the BlackBerry Device Service to complete the authentication process and configure an authenticated SRP connection
   - Rejects the challenge response

   If the BlackBerry Infrastructure rejects the challenge response, the authentication process is not successful. The BlackBerry Infrastructure and BlackBerry Device Service close the SRP connection.

   If the BlackBerry Device Service uses the same SRP authentication key and SRP identifier to connect to (and then disconnect from) the BlackBerry Infrastructure five times in one minute, the BlackBerry Infrastructure deactivates the SRP identifier to help prevent an attacker from using the SRP identifier to create conditions for a DoS attack.

How the BlackBerry Device Service protects a TCP/IP connection to the BlackBerry Infrastructure

After the BlackBerry Device Service and the BlackBerry Infrastructure open an SRP connection, the BlackBerry Device Service uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure.

The TCP/IP connection between the BlackBerry Device Service and BlackBerry Infrastructure is secure because the BlackBerry Device Service and device encrypt the data that they send to each other. No intermediate point decrypts and encrypts the data again.

After the activation process begins, no data traffic of any kind can occur between the BlackBerry Device Service and an activated device unless the BlackBerry Device Service can decrypt the data using a valid device transport key. Only the BlackBerry Device Service and the device have the correct device transport key.

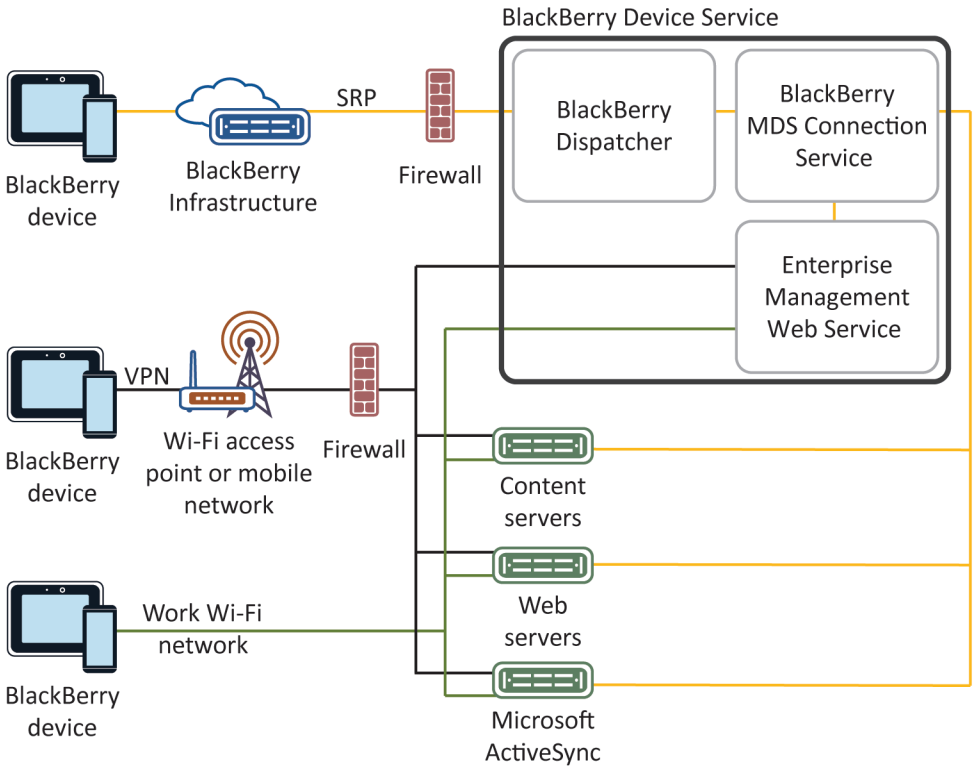
You must configure your organization's firewall or proxy server to permit the BlackBerry Device Service to start and maintain an outgoing connection to the BlackBerry Infrastructure over TCP port 3101.

How devices connect to the BlackBerry Device Service

3

Devices can connect to the BlackBerry Device Service and access your organization's network using a number of communication methods. By default, devices attempt to connect to your organization's network using the following communication methods, in order:

1. Work VPN profiles that you configure
2. Work Wi-Fi profiles that you configure
3. BlackBerry Infrastructure
4. Personal VPN profiles and personal Wi-Fi profiles that a user configures on the device



By default, the Enterprise Management Agent on the device can use all of these communication methods to connect to the BlackBerry Device Service and obtain the latest updates that you made to IT policies, profiles, software configurations, or IT administration commands.

By default, work apps on the device can also use any of these communication methods to access the resources in your organization's environment (for example, Microsoft ActiveSync servers, web servers, and content servers).

Related information

Controlling how work and personal apps connect to your organization's network, 57
Controlling the network connections that work and personal apps on BlackBerry PlayBook tablets can access, 71
Controlling app connections, 80

Types of encryption that devices use when they connect to your organization's resources

Devices and your organization's resources use tunneling to encapsulate various types of encryption. Tunneling occurs when data is encrypted using more than one layer of encryption. The type of encryption used depends on the type of connection between the device and the resource.

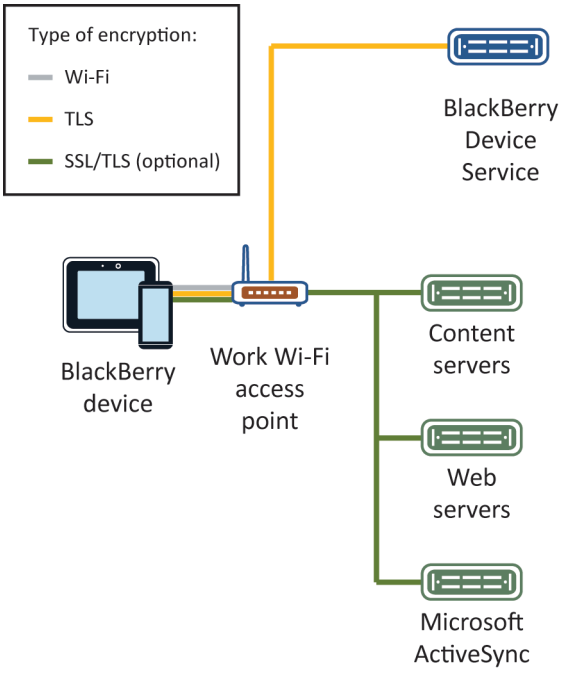
For example, in a work Wi-Fi connection, the data that a device and the BlackBerry Device Service send between each other is encrypted using SSL encryption. The data that the device and work wireless access point send to each other uses Wi-Fi encryption (unless the work wireless access point is an open network). Because the device uses tunneling, the data that the device sends to the BlackBerry Device Service is encrypted first by SSL encryption and then by Wi-Fi encryption as it travels between the device and the wireless access point.

Encryption type	Description
Wi-Fi encryption (IEEE 802.11)	Encrypts the data that is sent between the device and wireless access point if the wireless access point was set up to use Wi-Fi encryption.
VPN encryption	Encrypts the data that is sent between the device and VPN server.
TLS encryption	Encrypts the data that is sent between the device and BlackBerry Infrastructure. Encrypts the data that is sent between the device and BlackBerry Device Service. This type of encryption uses a client/server certificate.
SSL/TLS encryption	Encrypts the data that is sent between the device and content server, web server, or messaging server that uses Microsoft ActiveSync. The encryption for this connection must be set up separately on each server and uses a separate

Encryption type	Description
	certificate with each server. The server might use SSL or TLS, depending how it is set up.
AES encryption	Encrypts the data that is sent between the device and BlackBerry Device Service. This type of encryption uses the device transport key.

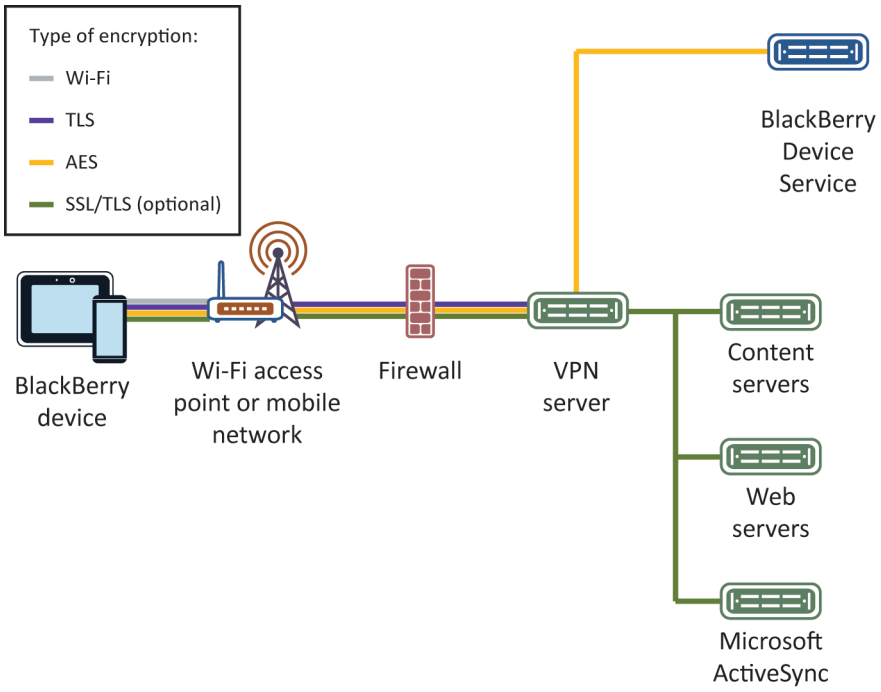
Work Wi-Fi connection

In a work Wi-Fi connection, a device connects to your organization's resources through a work Wi-Fi connection that you set up. Wi-Fi encryption is only used if the wireless access point was set up to use Wi-Fi encryption.



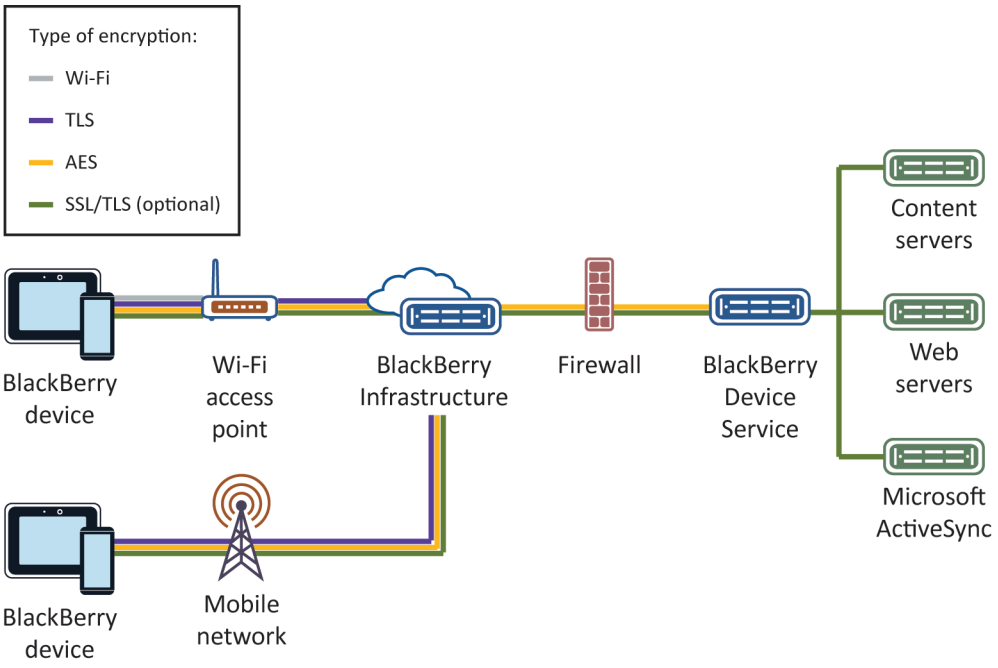
VPN connection

In a VPN connection, a device connects to your organization's resources through any wireless access point or a mobile network, your organization's firewall, and your organization's VPN server. Wi-Fi encryption is only used if the wireless access point was set up to use Wi-Fi encryption.



BlackBerry Infrastructure connection

In a BlackBerry Infrastructure connection, a device connects to your organization's resources through any wireless access point, the BlackBerry Infrastructure, your organization's firewall, and the BlackBerry Device Service. Wi-Fi encryption is only used if the wireless access point was set up to use Wi-Fi encryption.



Securing the communication between devices and your organization's network

Devices permit work apps and personal apps (on BlackBerry Balance devices) to use any of the Wi-Fi profiles or VPN profiles that are stored on the devices to connect to your organization's network. If you configure work Wi-Fi profiles or work VPN profiles using the BlackBerry Device Service, you permit personal apps on BlackBerry Balance devices to access your organization's network.

If the security requirements of your organization do not permit personal apps on BlackBerry Balance devices to access your organization's network, you can restrict connection options. You can use the "Work Network Usage for Personal Apps" IT policy rule to prevent personal apps on BlackBerry Balance devices (excluding BlackBerry PlayBook tablets) from using your organization's network to connect to the Internet using your work Wi-Fi network or work VPN connection.

You can also limit the communication methods that a device can use to connect to your organization's network through the BlackBerry Device Service by limiting connectivity options to the BlackBerry MDS Connection Service and the BlackBerry Infrastructure. Personal apps on BlackBerry Balance devices cannot use the BlackBerry MDS Connection Service and the BlackBerry Infrastructure to connect to your organization's network.

Related information

Controlling how work and personal apps connect to your organization's network, 57
Controlling the network connections that work and personal apps on BlackBerry PlayBook tablets can access, 71
Controlling app connections, 80

Using Kerberos to provide single sign-on from BlackBerry 10 devices

If your organization uses Kerberos to provide users with single sign-on access to your organization's resources, you can also provide users with single sign-on access to your organization's resources from the browser in the work space on their BlackBerry 10 devices.

When Kerberos is implemented within the BlackBerry Device Service, if a valid TGT is available on a user's device, the user is not prompted for credentials when accessing your organizations internal resources from the browser in the work space. If the user is connected to your organization using a VPN connection, the VPN gateway must permit traffic to the KDC to pass through for users to have access without providing credentials.

To use Kerberos with BlackBerry 10 devices, you specify your organization's Kerberos configuration file in the BlackBerry Administration Service.

For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

Protecting connections from a device to content servers and application servers

If an app on a BlackBerry 10 device can access servers on the Internet, you can configure the BlackBerry MDS Connection Service to use HTTPS to provide additional authentication and security for the connection. The device supports HTTPS in proxy mode using a proxy server or in direct mode using TLS.

If you configure HTTPS using TLS, the BlackBerry MDS Connection Service uses the TLS establishment algorithms, symmetric algorithms, and hash algorithms that the RIM Cryptographic API supports to open the connection for the device. The device uses TLS to encrypt data that an app sends to content servers. The BlackBerry MDS Connection Service does not decrypt data that it sends over the wireless network. You can use TLS when only the end points of the transaction are trusted (for example, with banking services).

How the BlackBerry Device Service manages email messages

Devices use Microsoft ActiveSync to synchronize email messages, calendar entries, and contacts with your organization's messaging server. The BlackBerry Device Service can allow devices that are not connected to your organization's internal network or do not have a VPN connection to synchronize with the messaging server without requiring you to make connections to Microsoft ActiveSync available from outside the firewall.

Microsoft ActiveSync can be configured to allow only connections with the BlackBerry Device Service. The BlackBerry Device Service allows devices to synchronize securely with the messaging server over the BlackBerry Infrastructure using the same encryption methods that it uses for all other work data. When the BlackBerry Device Service provides the connection between your messaging server and devices, the BlackBerry Device Service IT policies take precedence over any Microsoft ActiveSync policies that are set for the devices.

If your organization uses SCEP to enroll certificates to devices, you can associate a SCEP profile with an email profile to require certificate-based authentication to help protect connections between devices and the messaging server.

Related information

Extending messaging security on BlackBerry 10 devices, 85
Using SCEP to enroll client certificates to a device, 39

How devices can connect to the BlackBerry Infrastructure

Devices and the BlackBerry Infrastructure send all data to each other over a TLS connection. The TLS connection encrypts the data that devices and the BlackBerry Infrastructure send between each other.

A TLS connection between a device and the BlackBerry Infrastructure is designed so that an attacker cannot use the TLS connection to send data to or receive data from the device.

If an attacker tries to impersonate the BlackBerry Infrastructure, devices prevent the connection. Devices verify whether the public key of the TLS certificate of the BlackBerry Infrastructure matches the private key of the root certificate that is preloaded on the devices during the manufacturing process. If a user accepts a certificate that is not valid, the connection cannot open unless the device can also authenticate with a valid BlackBerry Device Service.

Data flow: Opening a TLS connection between the BlackBerry Infrastructure and a device

1. A device sends a request to the BlackBerry Infrastructure to open a TLS connection.
2. The BlackBerry Infrastructure sends its TLS certificate to the device.
3. The device uses a root certificate that is preloaded on the device to verify the TLS certificate. If the user deleted the root certificate, the device prompts the user to trust the TLS certificate.
4. The device opens the TLS connection.

Encrypting data that the BlackBerry Device Service and devices send to each other over the BlackBerry Infrastructure

To encrypt data that is in transit between the BlackBerry Device Service and devices in your organization, the BlackBerry Device Service and devices use BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data in transit over the BlackBerry Infrastructure.

Before the BlackBerry Device Service and devices send data to each other, they compress the data, encrypt the data using message keys, and encrypt the message keys using the device transport key. When the BlackBerry Device Service and devices receive data from each other, they decrypt the message keys using the device transport key, decrypt the data, and then decompress the data.

The BlackBerry Device Service and devices use AES-256 in CBC mode as the symmetric algorithm for BlackBerry transport layer encryption.

Device transport keys

The device transport key encrypts the message keys that help protect the data that is sent between the BlackBerry Device Service and devices. The BlackBerry Device Service and a device generate the device transport key when a user activates the device.

Only the BlackBerry Device Service and the device know the value of the device transport key. The BlackBerry Device Service and the device reject a data packet if they do not recognize the format of a data packet or do not recognize the device transport key that protects the data packet.

Devices store device transport keys in a keystore database in flash memory. The keystore database prevents an attacker from copying the device transport keys to a computer by trying to back up the device transport keys. An attacker cannot extract key data from flash memory.

The BlackBerry Device Service stores device transport keys in the BlackBerry Configuration Database. To avoid compromising the device transport keys that are stored in the BlackBerry Configuration Database, you must protect the BlackBerry Configuration Database.

Related information

Protecting the data that the BlackBerry Device Service stores in your organization's environment, 117

Generating the device transport key for a device

When you install the BlackBerry Device Service, the setup application creates an enterprise management root certificate and a server certificate for the BlackBerry Device Service. When a user activates a device, the device sends a CSR to the BlackBerry Device Service. The BlackBerry Device Service uses the CSR to create a client certificate, signs the client certificate with the enterprise management root certificate, and sends the client certificate and the enterprise management root certificate for the BlackBerry Device Service to the device. To protect the connection between the device and the BlackBerry Device Service during the certificate exchange, the device and the BlackBerry Device Service create a short-lived symmetric key using the activation password and EC-SPEKE.

When the certificate exchange is complete, the device and BlackBerry Device Service establish a mutually authenticated TLS connection using the client certificate and the server certificate. The device verifies the server certificate using the enterprise management root certificate.

To generate the device transport key, the device and the BlackBerry Device Service use the authenticated long-term public keys that are associated with the client certificate and with the server certificate for the BlackBerry Device Service, and ECMQV. The ECMQV protocol occurs over the mutually authenticated TLS connection. The elliptic curve used in ECMQV is the NIST-recommended 521-bit curve.

The BlackBerry Device Service and device do not send the device transport key over the wireless network when they generate the device transport key or when they exchange messages.

Message keys

The BlackBerry Device Service and a device generate one or more message keys that protect the integrity of the data (for example, short keys or large messages) that the BlackBerry Device Service and the device send between each other using the BlackBerry Infrastructure. If a message exceeds 2 KB and consists of several data packets, the BlackBerry Device Service and the device generate a unique message key for each data packet.

Each message key consists of random data that makes it difficult for a third party to decrypt, re-create, or duplicate the message key.

The BlackBerry Device Service and the device do not store the message keys in persistent storage. They free the memory that is associated with the message keys after the BlackBerry Device Service or device uses the message keys to decrypt the message.

The device uses the pseudorandom bits retrieved from the random source on the device to generate a message key.

Data flow: Generating a message key on a device

A device uses the DRBG function to generate a message key.

To generate a message key, the device performs the following actions:

1. Retrieves random data from multiple sources to generate the seed using a technique that the device derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array
3. Adds the 256-byte state array into the ARC4 encryption algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the ARC4 state array

   The device draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the call are not in the same place, and in case the first few bytes of the ARC4 state array are not random.
5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DRBG function

   The device stores a copy of the seed in a file. When the device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. Uses the DRBG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits to create the message key

For more information about the DRBG function, see *NIST Special Publication 800-90*.

Data flow: Generating a message key on the BlackBerry Device Service

A BlackBerry Device Service uses the DSA PRNG function to generate a message key.

To generate a message key, the BlackBerry Device Service performs the following actions:

1. Retrieves random data from multiple sources for the seed, using a technique that the BlackBerry Device Service derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array

   The BlackBerry Device Service requests 512 bits of randomness from the Microsoft Cryptographic API to increase the randomness of the data.
3. Adds the 256-byte state array into the ARC4 algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the 256-byte state array

   The BlackBerry Device Service draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the generation process are not in the same place, and in case the first few bytes of the 256-byte state array are not random.
5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DSA PRNG function

The BlackBerry Device Service stores a copy of the seed in a file. When the BlackBerry Device Service restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. Uses the DSA PRNG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits with AES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Using a VPN with a device

If your organization's environment includes VPNs, such as IPSec VPNs or SSL VPNs, you can configure a device to authenticate with the VPN so that it can access your organization's network. A VPN provides an encrypted tunnel between a device and your organization's network.

A VPN solution consists of a VPN client on the device and a VPN concentrator. The device can use the VPN client to authenticate with a VPN concentrator, which acts as the gateway to your organization's network. Each device includes a built-in VPN client that supports several VPN concentrators. The VPN client on the device uses strong encryption to authenticate itself with the VPN concentrator. It creates an encrypted tunnel between the device and VPN concentrator that the device and your organization's network can use to communicate.

For more information about configuring VPN profiles, see the *BlackBerry Device Service Advanced Administration Guide*.

Related information

VPN connection, 17

Protecting a connection between a device and a work Wi-Fi network

A device can connect to work Wi-Fi networks that use the IEEE 802.11 standard. The IEEE 802.11i standard uses the IEEE 802.1X standard for authentication and key management to protect work Wi-Fi networks. The IEEE 802.11i standard specifies that organizations must use the PSK protocol or the IEEE 802.1X standard as the access control method for Wi-Fi networks.

For more information about protecting a work Wi-Fi network, see the documentation from your organization's Wi-Fi solution provider.

How a device and the BlackBerry Device Service protect sensitive Wi-Fi information

To permit a device to access a Wi-Fi network, you must send sensitive Wi-Fi information such as encryption keys and passwords to the device using Wi-Fi profiles and VPN profiles. After the device receives the sensitive Wi-Fi information, the device encrypts the encryption keys and passwords and stores them in flash memory.

The BlackBerry Device Service encrypts the sensitive Wi-Fi information that it sends to the device and stores the sensitive Wi-Fi information in the BlackBerry Configuration Database. You can help protect the sensitive Wi-Fi information in the BlackBerry Configuration Database using access controls and configuration settings.

Layer 2 security methods that a device supports

You can configure a device to use security methods for layer 2 (also known as the IEEE 802.11 link layer) so that the wireless access point can authenticate the device and the device and the wireless access point can encrypt data that they send to each other. The device supports the following layer 2 security methods:

- WEP encryption (64-bit and 128-bit)
- IEEE 802.1X standard and EAP authentication using EAP-FAST, EAP-TLS, EAP-TTLS, and PEAP
- TKIP and AES-CCMP encryption for WPA-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise

To support layer 2 security methods, the device has a built-in IEEE 802.1X supplicant.

If a work Wi-Fi network uses EAP authentication, you can permit and deny device access to the work Wi-Fi network by updating your organization's central authentication server. You are not required to update the configuration of each access point.

For more information about IEEE 802.11 and IEEE 802.1X, see www.ieee.org/portal/site. For more information about EAP authentication, see RFC 3748.

IEEE 802.1X standard

The IEEE 802.1X standard defines a generic authentication framework that a device and a work Wi-Fi network can use for authentication. The EAP framework is specified in RFC 3748.

The device supports EAP authentication methods that meet the requirements of RFC 4017 to authenticate the device to the work Wi-Fi network. Some EAP authentication methods (for example, EAP-TLS, EAP-TTLS, EAP-FAST, or PEAP) use credentials to provide mutual authentication between the device and the work Wi-Fi network.

The device is compatible with the WPA-Enterprise and WPA2-Enterprise specifications.

Data flow: Authenticating a device with a work Wi-Fi network using the IEEE 802.1X standard

If you configured a wireless access point to use the IEEE 802.1X standard, the access point permits communication using EAP authentication only. This data flow assumes that you configured a device to use an EAP authentication method to communicate with the access point.

1. The device associates itself with the access point that you configured to use the IEEE 802.1X standard. The device sends its credentials (typically a username and password) to the access point.
2. The access point sends the credentials to the authentication server.
3. The authentication server performs the following actions:
   a Authenticates the device on behalf of the access point
   b Instructs the access point to permit access to the work Wi-Fi network
   c Sends Wi-Fi credentials to the device to permit it to authenticate with the access point
4. The access point and device use EAPoL-Key messages to generate encryption keys (for example, WEP, TKIP, or AES-CCMP, depending on the EAP authentication method that the device uses).

   When the device sends EAPoL messages, the device uses the encryption and integrity requirements that the EAP authentication method specifies. When the device sends EAPoL-Key messages, the device uses the ARC4 algorithm or AES algorithm to provide integrity and encryption.

After the access point and device generate the encryption key, the device can access the work Wi-Fi network.

EAP authentication methods that devices support

PEAP authentication

PEAP authentication permits devices to authenticate with an authentication server and access a work Wi-Fi network. PEAP authentication uses TLS to create an encrypted tunnel between a device and the authentication server. It uses the TLS tunnel to send the authentication credentials of the device to the authentication server.

Devices support PEAPv0 and PEAPv1 for PEAP authentication. Devices also support EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during PEAP authentication so that devices can exchange credentials with the work Wi-Fi network.

To configure PEAP authentication, you must install a root certificate on the device that corresponds to the authentication server certificate and install client certificates, if required. You can send root certificates to every device and you can use SCEP to enroll client certificates on devices.

For more information, see the *BlackBerry Device Service Advanced Administration Guide.*

EAP-TLS authentication

EAP-TLS authentication uses a PKI to permit a device to authenticate with an authentication server and access a work Wi-Fi network. EAP-TLS authentication uses TLS to create an encrypted tunnel between the device and the authentication

server. EAP-TLS authentication uses the TLS encrypted tunnel and a client certificate to send the credentials of the device to the authentication server.

Devices support EAP-TLS authentication when the authentication server and the client use certificates that meet specific requirements. To configure EAP-TLS authentication, you must install a client certificate and a root certificate on the device that corresponds to the certificate of the authentication server. You can use SCEP to enroll certificates on devices. For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

For more information about EAP-TLS authentication, see RFC 2716.

EAP-TTLS authentication

EAP-TTLS authentication extends EAP-TLS authentication to permit a device and an authentication server to mutually authenticate. When the authentication server uses its certificate to authenticate with the device and open a protected connection to the device, the authentication server uses an authentication protocol over the protected connection to authenticate with the device.

Devices support EAP-MS-CHAPv2, MS-CHAPv2, and PAP as second-phase protocols during EAP-TTLS authentication so that devices can exchange credentials with the work Wi-Fi network. If you want to use PAP as a second-phase protocol, you must set the EAP Inner Link Security profile setting to Auto.

To configure EAP-TTLS authentication, you must install the root certificate on the device that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

EAP-FAST authentication

EAP-FAST authentication uses PAC to open a TLS connection to a device and verify the supplicant credentials of the device over the TLS connection.

Devices support EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during EAP-FAST authentication so that devices can exchange authentication credentials with work Wi-Fi networks. Devices support the use of automatic PAC provisioning with EAP-FAST authentication only.

For more information about EAP-FAST authentication, see RFC 4851.

EAP authentication methods that devices support the use of CCKM with

Devices support the use of CCKM with all supported EAP authentication methods to improve roaming between wireless access points. Devices do not support the use of CCKM with the Cisco CKIP encryption algorithm or the AES-CCMP encryption algorithm.

Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication

If your organization uses PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to protect the wireless access points for a work Wi-Fi network, a device must authenticate mutually with an access point using an authentication server. To generate the certificates that the device and authentication server use to authenticate with each other, you require a CA.

For PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to be successful, the device must trust the certificate of the authentication server. The device does not trust the certificate of the authentication server automatically. Before you can configure the device to trust the certificate of the authentication server, the following conditions must exist:

- A CA that the device and authentication server mutually trust must generate the certificate of the authentication server and a certificate for the device.
- The device must store the root certificates in the certificate chain for the certificate of the authentication server.

Each device stores a list of root certificates that are issued by CAs that it explicitly trusts.

You can send root certificates to every device and you can use SCEP to enroll client certificates on devices. For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

Activating devices

4

When you or a user activates a device, you create the work space on the device, associate the work space with a user account in the BlackBerry Device Service, and establish a secure communication channel between the device and the BlackBerry Device Service.

The BlackBerry Device Service allows multiple devices to be activated for the same user account. More than one active BlackBerry 10 device and more than one active BlackBerry PlayBook tablet can be associated with a user account.

Devices can be activated to use BlackBerry Balance technology or to have a work space only. Only devices with BlackBerry 10 OS version 10.1 and later that have an appropriate service plan can be activated to have a work space only. If you or a user attempts a work space only activation of device that does not support it, the device will not activate correctly and it will not be able to access your organization's data.

You can activate a device for a user by logging into the BlackBerry Administration Service and connecting the device to the computer. You can also configure how users can activate devices and whether you can use the BlackBerry Device Service to send activation passwords and instructions to a user's work email account.

A user can activate a device by connecting the device to their computer and logging into the BlackBerry Web Desktop Manager. By default, a user can also activate a device wirelessly using any of the following connections:

- Over your work Wi-Fi network
- Over any Wi-Fi connection or mobile network using a VPN connection
- Over any Wi-Fi connection or mobile network through the BlackBerry Infrastructure

When the activation process completes, the BlackBerry Device Service can send apps, profiles, IT policies, and wallpaper image files to the device and, if email profiles are configured, users can send and receive work email messages using the device.

Activating a device over a wireless connection

You can allow a user to activate a device over a wireless connection using the following methods:

- A work Wi-Fi connection or a VPN connection to the Enterprise Management Web Service
- Any Wi-Fi connection or mobile network connection through the BlackBerry Infrastructure

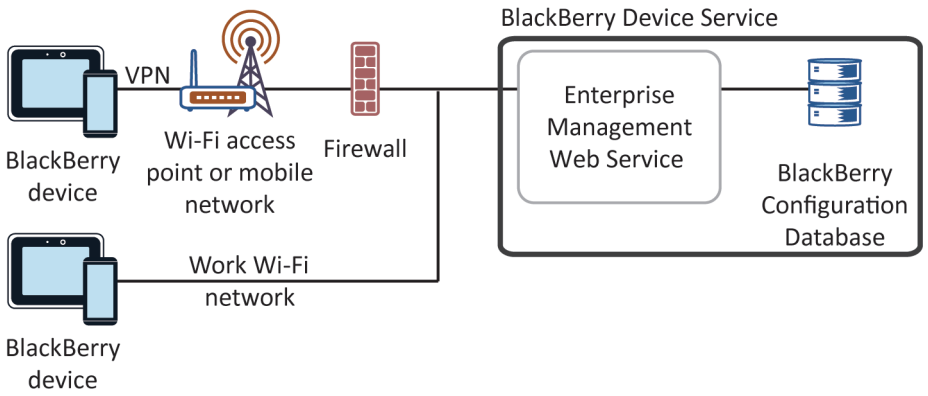
You can configure the wireless activation settings in the BlackBerry Administration Service to prevent a user from activating a device using the BlackBerry Infrastructure. You can also register your organization's activation information with

the BlackBerry Infrastructure. If you register the activation information, the user's account information, including their username, activation password, required server address and SRP information will be sent to and stored in the BlackBerry Infrastructure. Users who activate a BlackBerry 10 device will not need to know the SRP ID of the BlackBerry Device Service and will only need to provide their work email address and activation password to activate a device.

When a user begins activation of a BlackBerry Balance device, if the device has an existing work space, the device displays a warning message to indicate that the work data and work apps on the device will be deleted. When the user confirms that the device should be activated, the existing work space is deleted and a new work space is created.

When a user begins activation of a work space only device, the device displays a warning message to indicate that all data on the device will be deleted. When the user confirms that the device should be activated, all data is deleted and the device restarts before the new work space is created.

Data flow: Activating a device over a work Wi-Fi connection or a VPN connection



1. You perform the following actions:
   a. Add a user account to the BlackBerry Device Service using the account information retrieved from your organization's Microsoft Active Directory
   b. Set the user's activation type to either BlackBerry Balance or work space only
   c. Create an activation password for the user account
   d. Communicate the password and the Enterprise Management Web Service web address to the user
2. The user performs the following actions:

a Types the user ID, activation password, and the Enterprise Management Web Service web address (if necessary) on the device

b For a work space only activation, accepts the organization notice, which outlines the terms and conditions that the user must agree to.

3. If the activation is a work space only activation, the device deletes all existing data and restarts.
4. The Enterprise Management Agent on the device performs the following actions:
   a Establishes a connection to the Enterprise Management Web Service
   b Sends an activation request to the Enterprise Management Web Service
   c Creates the work space on the device
5. The Enterprise Management Agent and Enterprise Management Web Service generate a shared symmetric key using the activation password and EC-SPEKE. The shared symmetric key is designed to help protect the CSR and response.
6. The Enterprise Management Agent performs the following actions:
   a Generates a key pair for the certificate
   b Creates a PKCS#10 CSR that includes the public key of the key pair
   c Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
   d Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR
   e Sends the encrypted CSR and HMAC to the Enterprise Management Web Service
7. The Enterprise Management Web Service performs the following actions:
   a Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
   b Retrieves the user ID, work space ID, device PIN, and your organization's name from the BlackBerry Configuration Database
   c Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent
   d Signs the client certificate using the enterprise management root certificate
   e Encrypts the client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
   f Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL and appends it to the encrypted data
   g Sends the encrypted data and HMAC to the Enterprise Management Agent
8. The Enterprise Management Agent performs the following actions:
   a Verifies the HMAC
   b Decrypts the data it received from the Enterprise Management Web Service
   c Stores the client certificate and the enterprise management root certificate in its keystore
9. The Enterprise Management Agent and Enterprise Management Web Service perform the following actions:

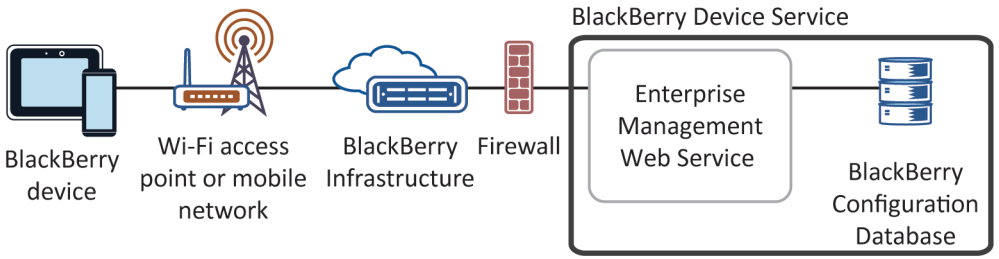
a Establish a mutually authenticated TLS connection by verifying both the client certificate and the server certificate for the Enterprise Management Web Service using the enterprise management root certificate

b Generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for the Enterprise Management Web Service

10. The Enterprise Management Agent stores the device transport key in its keystore.
11. The Enterprise Management Web Service performs the following actions:
    a Stores the device transport key in the BlackBerry Configuration Database
    b Sends the IT policy, SRP information, profiles, and software configurations to the device over TLS
12. The Enterprise Management Agent sends an acknowledgment that it received the IT policy and other data to the Enterprise Management Web Service over TLS. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

Data flow: Activating a device over a connection to the BlackBerry Infrastructure



1. You perform the following actions:
    a Add a user account to the BlackBerry Device Service using the account information retrieved from your organization's Microsoft Active Directory
    b Set the user's activation type to either BlackBerry Balance or work space only
    c Create an activation password for the user account
    d Communicate the password and, if necessary, the SRP ID of the BlackBerry Device Service to the user
2. The user performs the following actions:
    a Types the user ID, activation password, and SRP ID of the BlackBerry Device Service (if necessary) on the device

   b For a work space only activation, accepts the organization notice, which outlines the terms and conditions that the user must agree to

3. If the activation is a work space only activation, the device deletes all existing data and restarts.
4. The Enterprise Management Agent on the device establishes a connection through the BlackBerry Infrastructure to the BlackBerry Device Service.
5. The BlackBerry MDS Connection Service receives the activation request and sends the Enterprise Management Web Service host and port information back to the Enterprise Management Agent.
6. The Enterprise Management Agent on the device performs the following actions:
   a Establishes a connection to the Enterprise Management Web Service through the BlackBerry MDS Connection Service
   b Sends an activation request to the Enterprise Management Web Service
   c Creates the work space on the device
7. The Enterprise Management Agent and Enterprise Management Web Service generate a shared symmetric key from the activation password using EC-SPEKE. The shared symmetric key is designed to help protect the CSR and response.
8. The Enterprise Management Agent performs the following actions:
   a Generates a key pair for the certificate
   b Creates a PKCS#10 CSR that includes the public key of the key pair
   c Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
   d Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR
   e Sends the encrypted CSR and HMAC to the Enterprise Management Web Service
9. The Enterprise Management Web Service performs the following actions:
   a Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
   b Retrieves the user ID, work space ID, device PIN, and your organization's name from the BlackBerry Configuration Database
   c Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent
   d Signs the client certificate using the enterprise management root certificate
   e Encrypts the client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
   f Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL and appends it to the encrypted data
   g Sends the encrypted data and HMAC to the Enterprise Management Agent
10. The Enterprise Management Agent performs the following actions:
   a Verifies the HMAC
   b Decrypts the data it received from the Enterprise Management Web Service

c Stores the client certificate and the enterprise management root certificate in its keystore

11. The Enterprise Management Agent and Enterprise Management Web Service perform the following actions:
    a Establish a mutually authenticated TLS connection by verifying both the client certificate and the server certificate for the Enterprise Management Web Service using the enterprise management root certificate
    b Generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for the Enterprise Management Web Service
12. The Enterprise Management Agent stores the device transport key in its keystore.
13. The Enterprise Management Web Service performs the following actions:
    a Stores the device transport key in the BlackBerry Configuration Database
    b Sends the IT policy, SRP information, profiles, and software configurations to the device over TLS
14. The Enterprise Management Agent sends an acknowledgment that it received the IT policy and other data to the Enterprise Management Web Service over TLS. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

Activating a device using the BlackBerry Web Desktop Manager

A user can activate a new device, reactivate an existing device, or switch services from one device to another device by connecting the device to a computer using a USB cable and logging in to the BlackBerry Web Desktop Manager.

When a user begins activation of a BlackBerry Balance device, if the device has an existing work space, the BlackBerry Web Desktop Manager displays a warning message to indicate that the work data and work apps on the device will be deleted. When the user confirms that the device should be activated, the existing work space is deleted and a new work space is created.

When a user begins activation of a work space only device, the BlackBerry Web Desktop Manager displays a warning message to indicate that all data on the device will be deleted. When the user confirms that the device should be activated, all data is deleted and the device restarts before the new work space is created.

For more information, see the *BlackBerry Web Desktop Manager User Guide*.

Data flow: Activating a device using the BlackBerry Web Desktop Manager

1. You perform the following actions:
   a. Add a user account to the BlackBerry Device Service using the account information retrieved from your organization's Microsoft Active Directory
   b. Set the user's activation type to either BlackBerry Balance or work space only
2. A user performs the following actions:
   a. Connects a device to a computer using a USB cable
   b. On the computer, browses to the BlackBerry Web Desktop Manager using Windows Internet Explorer and logs in
3. If necessary, the browser downloads and installs the BlackBerry device communication components. The BlackBerry device communication components are Microsoft ActiveX controls that permit the BlackBerry Device Service to communicate with a tethered device.
4. The BlackBerry device communication components send the device PIN to the BlackBerry Device Service over an HTTPS connection to start the activation process.
5. The BlackBerry Device Service receives the device PIN and performs the following actions:
   a. Stores the device PIN in the BlackBerry Configuration Database
   b. Generates an activation password. You and the user cannot view the activation password
   c. Sends the activation password, user ID, and the server name and port of the Enterprise Management Web Service to the Enterprise Management Agent
6. If the activation is a work space only activation, the user accepts the organization notice, which outlines the terms and conditions that the user must agree to.
7. If the activation is a work space only activation, the device deletes all existing data and restarts.
8. The Enterprise Management Agent creates the work space on the device.
9. The Enterprise Management Agent and Enterprise Management Web Service generate a shared symmetric key from the activation password using EC-SPEKE. The shared symmetric key is designed to help protect the CSR and response.
10. The Enterprise Management Agent performs the following actions:
    a. Generates a key pair for the certificate
    b. Creates a PKCS#10 CSR that includes the public key of the key pair
    c. Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
    d. Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR

e Sends the encrypted CSR and HMAC to the Enterprise Management Web Service

11. The Enterprise Management Web Service performs the following actions:
    a Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
    b Retrieves the user ID, work space ID, device PIN, and your organization's name from the BlackBerry Configuration Database
    c Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent
    d Signs the client certificate using the enterprise management root certificate
    e Encrypts the client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
    f Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL and appends it to the encrypted data
    g Sends the encrypted data and HMAC to the Enterprise Management Agent
12. The Enterprise Management Agent performs the following actions:
    a Verifies the HMAC
    b Decrypts the data it received from the Enterprise Management Web Service
    c Stores the client certificate and the enterprise management root certificate in its keystore
13. The Enterprise Management Agent and Enterprise Management Web Service perform the following actions:
    a Establish a mutually authenticated TLS connection by verifying both the client certificate and the server certificate for the Enterprise Management Web Service using the enterprise management root certificate
    b Generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for the Enterprise Management Web Service
14. The Enterprise Management Agent stores the device transport key in its keystore.
15. The Enterprise Management Web Service performs the following actions:
    a Stores the device transport key in the BlackBerry Configuration Database
    b Sends the IT policy, SRP information, profiles, and software configurations to the device over TLS
16. The Enterprise Management Agent sends an acknowledgment that it received the IT policy and other data to the Enterprise Management Web Service over TLS. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

Managing certificates on devices

5

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that is stored separately. A CA signs the certificate to verify that it can be trusted.

Devices can use certificates to:

- Authenticate using SSL/TLS when it connects to web pages that use HTTPS
- Authenticate with a work messaging server
- Authenticate with a work Wi-Fi network or VPN
- Encrypt and sign email messages using S/MIME protection (BlackBerry 10 devices only)

Many certificates used for different purposes can be stored on a device. The BlackBerry Device Service sends certificates to devices during the activation process. You can also use SCEP profiles to enroll client certificates to devices and you can send server certificates and root certificates to all devices managed by the BlackBerry Device Service. If users have the BlackBerry Smart Card Reader 2.0 and BlackBerry 10 version 10.1 devices, users can also import S/MIME certificates to the device from a smart card.

Related information

S/MIME certificates and S/MIME private keys on BlackBerry 10 devices, 89
BlackBerry Smart Card Reader, 104

Certificates that the BlackBerry Device Service and a device use to authenticate with each other

When you install the BlackBerry Device Service, the setup application creates an enterprise management root certificate. The BlackBerry Device Service uses the enterprise management root certificate for the following purposes:

- To sign a server certificate for the Enterprise Management Web Service component
- To sign client certificates for devices

- To set up a TLS connection between the BlackBerry Device Service and a device so that the BlackBerry Device Service can activate the device and send management commands to it

The BlackBerry Device Service setup application creates the server certificate during the installation process.

When a user activates a device, the device generates a key pair and sends the public key to the BlackBerry Device Service in a CSR. The BlackBerry Device Service creates a client certificate and sends the enterprise management root certificate and client certificate to the device. The BlackBerry Device Service and device automatically renew the client certificate when it expires after one year.

The device uses the enterprise management root certificate to verify the server certificate for the Enterprise Management Web Service. The BlackBerry Device Service and the device use the client certificate to authenticate the user, work space, and device.

Related information

Data flow: Activating a device over a work Wi-Fi connection or a VPN connection, 31
Data flow: Activating a device over a connection to the BlackBerry Infrastructure, 33
Data flow: Activating a device using the BlackBerry Web Desktop Manager, 36

Using SCEP to enroll client certificates to a device

SCEP is an IETF protocol that simplifies the process of enrolling certificates to a large number of users. Devices can connect to any SCEP compliant CA, such as a Microsoft CA, using SCEP. The devices can use SCEP to connect to the CA that is used by your organization and obtain any required client certificates.

You can use SCEP to enroll client certificates to devices so that the devices can connect to a work Wi-Fi network, work VPN network, or work messaging server using Microsoft ActiveSync. Certificate enrollment starts after a device receives a Wi-Fi profile, VPN profile, or email profile that has an associated SCEP profile that you configured using the BlackBerry Device Service. Devices can receive a SCEP profile from the BlackBerry Device Service during the activation process, when you change a SCEP profile, or when you change another profile that has an associated SCEP profile. After the certificate enrollment completes, the client certificate and its certificate chain and private key are stored in the work keystore on the device.

The CA that you use must support challenge passwords. You set the challenge password in the SCEP profile. All devices that use the SCEP profile use the same challenge password. To help protect this password, the password is not sent to the devices.

For more information about SCEP, visit www.ietf.org.

Managing certificates that a device enrolls using SCEP

After a device enrolls a certificate using SCEP, the SCEP component monitors the expiry date and revocation status of the certificate. When the expiry date of a certificate approaches, the SCEP component starts the enrollment process for a new

certificate. You can use the Automatic Renewal SCEP profile setting to configure how many days before the certificate expires that automatic renewal occurs.

The certificate enrollment process can also start again if you change any of the following SCEP profile settings:

- Certification Authority Identifier
- Certificate Thumbprint
- Key Algorithm
- ECC Strength
- RSA Strength

The certificate enrollment process does not delete the existing certificate from the device or notify the CA that the certificate is no longer in use. If a SCEP profile is removed from the BlackBerry Device Service, the corresponding certificate is not removed from the device.

Data flow: Enrolling a client certificate to a device using SCEP

1. The BlackBerry Device Service sends a Wi-Fi profile, VPN profile, or email profile that has an associated SCEP profile to the device.
2. The device performs the following actions:
   a Generates a key pair using the key algorithm and strength that is specified in the SCEP profile
   b Generates a PKCS#10 CSR containing all required attributes for the request, except for the challenge password
   c Sends the SCEP profile name, PKCS#10 CSR, and hash type to the Enterprise Management Web Service
3. The Enterprise Management Web Service performs the following actions:
   a Verifies that the subject distinguished name, subject alternative names, and email address that are contained in the request match the user account information in the BlackBerry Configuration Database
   b Adds the challenge password to the PKCS#10 CSR
   c Hashes the PKCS#10 CSR
   d Sends the PKCS#10 CSR hash to the device
4. The device computes the signature on the PKCS#10 CSR hash, and sends the SCEP profile name, original PKCS#10 CSR, signature request, computed signature response, CA certificate (to encrypt the SCEP request), hash type, and encryption type to the Enterprise Management Web Service.
5. The Enterprise Management Web Service performs the following actions:
   a Verifies the CA certificate that it receives
   b Verifies that the subject distinguished name, subject alternative names, and email address that are contained in the request match the user account information in the BlackBerry Configuration Database
   c Adds the challenge password to the PKCS#10 CSR

d Adds the computed signature response to the PKCS#10 CSR

e Encrypts the PKCS#10 CSR using PKCS#7 enveloped data format and the CA public key

f Sends the PKCS#7 enveloped data to the device

6. The device completes the SCEP request by signing the PKCS#7 enveloped data using PKCS#7 signed data format and sends the SCEP request to the CA.
7. The CA issues the certificate and sends it to the device.
8. The Enterprise Management Agent on the device adds the certificate and corresponding private key to the keystore on the device.

Sending CA certificates to devices

You might need to distribute root and intermediate CA certificates to devices if the devices use certificate-based authentication to connect to a network or server in your organization's environment or if your organization uses S/MIME.

Sending the CA certificates for your organization's network and server certificates to devices allows the devices to trust the network and servers when making secure connections. Sending CA certificates for your organization's S/MIME certificates allows devices to trust the sender's certificate when a secure email message is received.

You can send CA certificates to every device that is managed by the BlackBerry Device Service by copying the certificate to the appropriate subfolder in the BlackBerry Device Service shared network folder. If the contents of a certificate folder change, the Enterprise Management Web Service sends all certificates in the folder to the appropriate certificate store on every device to replace the previous set of certificates.

Depending on the purpose of a certificate, you should copy a CA certificate to one of the following Certificates subfolders:

Folder	Description
WIFI	The BlackBerry Device Service sends certificates in the WIFI folder to the Wi-Fi Trusted Certificates store on every device. Certificates in the Wi-Fi Trusted Certificates store can be used only for Wi-Fi connections. You must set the Wi-Fi profile Trusted Certificate Source configuration setting to Trusted Certificate Store to use certificates in the store for work Wi-Fi connections.
VPN	The BlackBerry Device Service sends certificates in the VPN folder to the VPN Trusted Certificates store on every device. Certificates in the VPN Trusted Certificates store can be used only for VPN connections. You must set the VPN profile Trusted Certificate Source configuration setting to Trusted Certificate Store to use certificates in the store for work VPN connections.
WWW	The BlackBerry Device Service sends certificates in the WWW folder to the Enterprise Root Certificates list on every device. The work browser uses these certificates to establish SSL connections with servers in your organization's environment.

Folder	Description
	Devices running BlackBerry 10 OS version 10.0 also use certificates in this folder to authenticate with your work messaging server if it uses certificate-based authentication and to authenticate secure email messages that have been received.
Enterprise	The BlackBerry Device Service sends certificates in the Enterprise folder to the Enterprise Root Certificates list on devices running BlackBerry 10 OS version 10.1 and later. Devices use certificates in this folder to authenticate with your work messaging server if it uses certificate-based authentication and to authenticate secure email messages that have been received.

For more information about sending CA certificates to devices, see the *BlackBerry Device Service Advanced Administration Guide*.

Using IT policies to manage BlackBerry Device Service security

6

You can use IT policies to control and manage devices in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Device Service solution. For example, you can use IT policy rules to manage the following security features and behaviors of the device:

- Use of a password
- Connections that use Bluetooth wireless technology
- Availability of certain apps and device features

The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device.

After a user activates a device, the BlackBerry Device Service automatically sends to the device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Device Service sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Device Service automatically reassigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Device Service Policy and Profile Reference Guide.*

Preconfigured IT policy

The BlackBerry Device Service includes the following preconfigured IT policy. You can change the preconfigured IT policy to meet the requirements of your organization or copy this IT policy to create new IT policies.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set on the BlackBerry Device Service.

Resolving IT policy conflicts

If you add a user account to multiple groups, multiple IT policies can be added to the user account. You can control how the BlackBerry Device Service applies the correct IT policies and IT policy rules to the user account.

The BlackBerry Device Service applies the IT policy that you assign directly to the user account first.

If you do not assign an IT policy directly to the user account, the BlackBerry Device Service applies the IT policies that you assign to the group using one of the following methods:

Method	Description
Apply one IT policy to a user account	You can configure the BlackBerry Device Service to apply only one IT policy to a user account. If you select this method to resolve IT policy conflicts, the BlackBerry Device Service applies the IT policy with the highest ranking in the BlackBerry Administration Service.
Apply multiple IT policies to a user account	You can configure the BlackBerry Device Service to apply multiple IT policies to a user account. If you select this method to resolve IT policy conflicts, the BlackBerry Device Service combines the IT policies into one IT policy and applies it to the user account. A conflict occurs when you change an IT policy rule from the default value to different values in different IT policies. If there is a conflict between IT policy rules in different IT policies, the BlackBerry Device Service uses the IT policy rule from the IT policy with the highest ranking in the BlackBerry Administration Service.

7 Using BlackBerry Balance to secure BlackBerry 10 devices in your organization's environment for work use and personal use

Your organization can use BlackBerry Balance technology to permit users to use BlackBerry 10 devices for both work and personal use. For example, your organization might want to permit users to activate their personal devices on the BlackBerry Device Service or permit users to use devices that your organization provides for personal use.

The BlackBerry Device Service security features and BlackBerry Balance can control how devices protect your organization's content and resources (data, apps, and network connections) and allow devices to treat your organization's data and apps differently from personal data and apps. These features and options have the following benefits:

- Permit your organization to control access to your organization's data and apps on devices
- Help prevent your organization's data from being compromised
- Provide a unified experience for users when they access personal data and work data within some core apps
- Permit you to install and manage your organization's apps on devices
- Permit you to delete your organization's data and apps from personal devices when users are no longer a part of your organization
- Permit you to control network connections for work and personal apps

BlackBerry Balance is designed to separate and secure work and personal information on devices running BlackBerry 10 OS that are activated on the BlackBerry Device Service. BlackBerry Balance uses separate areas of the device called spaces to separate work and personal activities. A space is a distinct area of the device that enables the segregation and management of different types of data, apps, and network connections. Different spaces can have different rules for data storage, app permissions, and network routing. The separate spaces help users to avoid activities such as accidentally copying work data into a personal app, or displaying confidential work data during a BBM Video chat.

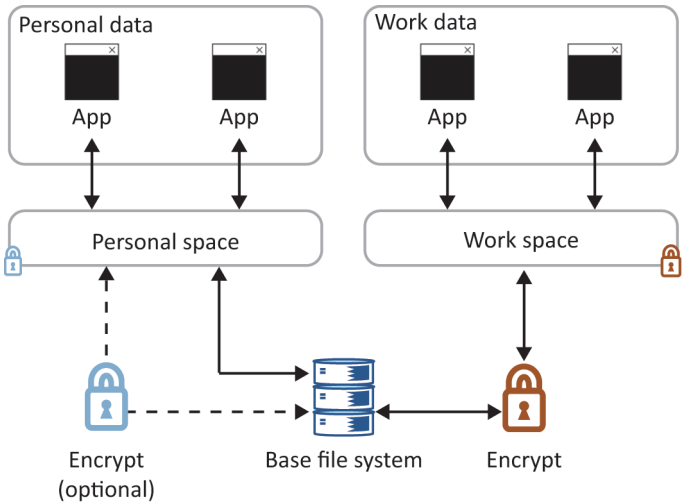
The device encrypts the work space during the activation process. You can use an IT policy rule to require the device to encrypt the personal space separately.

Devices that are not activated on the BlackBerry Device Service operate only a personal space. When you activate a device on the BlackBerry Device Service using the BlackBerry Balance option, a work space is created on the device. The personal space on the device remains intact during the activation process and any user data, apps, or network connections

that the user was using before the device was activated on the BlackBerry Device Service are available to the user in the personal space on the device.

Retaining the original personal space on the device provides users with the opportunity to use devices for activities that your organization's security policies might not otherwise allow, such as downloading videos, playing online multi-player games, and uploading personal photos and Facebook entries, without exposing your organization's content that is stored in the work space.

The work space is a segregated area of the device for work resources that also provides a modified version of the BlackBerry World storefront called BlackBerry World for Work. BlackBerry World for Work contains the apps that your organization allows users to download and use at work. The work space also provides a segregated area of the device where users can create, edit, and save work documents and slide decks.



Securing work and personal data and apps on devices

Security features on both the BlackBerry Device Service and BlackBerry Balance devices running BlackBerry 10 help to classify, protect, and manage work and personal data and apps on devices.

How devices classify work and personal data and apps

BlackBerry Balance devices running BlackBerry 10 can distinguish between data that is for work use and data that is for personal use. Devices classify data as work data or personal data based on the source of the data, and these classifications determine how devices store, protect, and handle data on devices. For example, if data comes from a work account, it is stored in the work space on the device, and if data comes from a personal account, it is stored in the personal space on the device. After devices classify data as work data or personal data, personal data cannot be reclassified as work data and work data cannot be reclassified as personal data.

How devices classify data and apps

BlackBerry Balance devices running BlackBerry 10 classify work data as any data that is managed by apps in the work space and personal data as any data that is managed by apps in the personal space.

The following table describes each app classification and lists examples of apps that belong to each app classification:

Description	App
Apps that are available only in the work space and display only work data	• BlackBerry World for Work • Any apps deployed by your organization • Any apps that users download from BlackBerry World for Work
Apps that are available only in the personal space and that display only personal data	• BBM (with access to work contacts except if prevented by the "Personal Apps Access to Work Contacts" IT policy rule) • BBM Video (with access to work contacts except if prevented by the "Personal Apps Access to Work Contacts" IT policy rule) • BlackBerry Newsstand • BlackBerry Story Maker • BlackBerry World • Calculator • Camera • Compass • Consumer Instant Messaging Apps • Facebook for BlackBerry devices • Phone

Description	App
	• SMS text messaging (with access to work contacts except if prevented by the "Personal Apps Access to Work Contacts" IT policy rule) • Visual voice mail (with access to work contacts except if prevented by the "Personal Apps Access to Work Contacts" IT policy rule) • Weather • Any apps that users download from BlackBerry World (including BlackBerry Runtime for Android apps)
Apps that are available in both the work space and the personal space and display work data and personal data in a unified view These apps classify the data that they use as either work or personal data based on the source of the data and manage each type of data within the space that it belongs to. For example, the BlackBerry Hub, Calendar, Contacts, BlackBerry Remember app, and the universal search manage work data within the restrictions of the work file system, policies, permissions, and rules to ensure that the data is secured inside the work space and no data is available to users when the work space is locked. These apps are strictly controlled and limited to core apps that are developed by Research In Motion only.	• BlackBerry Remember • BlackBerry Hub • Calendar • Contacts • Search
Apps that have one instance in the work space and a separate instance in the personal space These app instances operate independently in both the work space and the personal space on devices. For example, the Documents To Go app that is located in the work space can manage only files that are located in the work space and the BlackBerry 10 OS prevents this app from interacting with files that are located in the personal space. Each instance of these apps is kept separate from the other, and each app operates under the rules and restrictions that apply to the space it is installed in. For example, the File Manager app displays only work files when a user opens the app in the work space and displays only personal files when the user opens the app in the personal space.	• Adobe Reader • Browser • Documents To Go • File Manager • Help • Music • Pictures • Print To Go • Videos

How devices are designed to prevent BlackBerry Runtime for Android apps from accessing work data and apps

BlackBerry Balance devices running BlackBerry 10 classify Android apps as personal apps and as such, they can be installed only in the personal space on devices. You cannot deploy or approve Android apps for installation in the work space. Android apps can access only personal data that is located in the personal space. Android apps do not have access to the work apps or work data that are located in the work space.

How the BlackBerry Device Service and devices protect work and personal data and apps

BlackBerry Balance devices running BlackBerry 10 protect work data by encrypting the files stored in the work space. Devices can also protect personal data by encrypting the files stored in the personal space if you or a user requires. Devices can also encrypt the files stored on media cards that are inserted in devices; only personal data can be saved to media cards. Devices encrypt only the contents of files; file and directory names are not encrypted.

You can protect work data on devices further by requiring password protection and controlling when devices wipe their work space.

Related information

Protecting data, 92

How devices protect work data

BlackBerry Balance devices running BlackBerry 10 encrypt data stored in the work file system using XTS-AES-256.

A device randomly generates an encryption key to encrypt the contents of a file. The file encryption keys are protected by a hierarchical system of encryption keys as follows:

- The device encrypts the file encryption key with the work domain key and stores the encrypted file encryption key as a metadata attribute of the file
- The work domain key is a randomly generated key that is stored in the file system metadata and is encrypted using the work master key
- The work master key is also randomly generated. The work master key is stored in NVRAM on the device and is encrypted with the system master key
- The system master key is stored in the replay protected memory block on the device
- The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured

The file encryption keys, the work domain key, the work master key, and the system master key are generated using the BlackBerry OS Cryptographic Kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS.

How devices protect personal data

BlackBerry Balance devices running BlackBerry 10 allow the encryption of personal files on devices.

You can use the "Personal Space Data Encryption" IT policy rule to turn on encryption for the personal space of devices. If the "Personal Space Data Encryption" rule is set to Yes, files stored in the personal space of the device are encrypted. If this rule is set to No, users can choose to encrypt files in the personal space using the Device Encryption option in the Security and Privacy settings on the device.

If encryption is turned on for the personal space of the device, the device encrypts files stored in the personal file system using XTS-AES-256. A device randomly generates an encryption key to encrypt the contents of a file. The file encryption keys are protected by a hierarchical system of encryption keys, as follows:

- The device encrypts the file encryption key with the personal domain key and stores the encrypted file encryption key as a metadata attribute of the file
- The personal domain key is a randomly generated key that is stored in the file system metadata and is encrypted using the personal master key
- The personal master key is also randomly generated. The personal master key is stored in NVRAM on the device and is encrypted with the system master key
- The system master key is stored in the replay protected memory block on the device
- The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured

If you set the "Personal Space Data Encryption" IT policy rule to Yes, you should also set the "Apply Work Space Password to Full Device" IT policy rule to Yes so that the work space password applies to the entire device. If you set the "Personal Space Data Encryption" IT policy rule to No and the user chooses to turn on encryption for the personal space, the device prompts the user to type a new password if the device does not already have a password.

Devices can also encrypt all files stored on media cards that are inserted in devices. Users can save only personal data to media cards.

The file encryption keys, the personal domain key, the personal master key, and the system master key are generated using the BlackBerry OS Cryptographic Kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS.

Related information

Protecting data on media cards, 50

Protecting data on media cards

BlackBerry Balance devices running BlackBerry 10 allow users to store only personal data on media cards and that data is stored in an unencrypted format.

Although users can't move or save work files to media cards, if your organization wants to ensure the security of files on them, you can require that devices encrypt all files stored on them using the "Media Card Encryption" IT policy rule.

Related information

Media cards, 103

Protecting work data on devices with password rules

To secure work content and resources in the work space, when BlackBerry 10 devices are activated on the BlackBerry Device Service using the BlackBerry Balance option, devices require users to set a password for the work space by default. If you don't want users to have to enter a password to access work content and resources in the work space, you can set the "Password Required for Work Space" IT policy rule to No.

You can use IT policy rules to enforce either a password for the work space or the entire device and then control password requirements for that password, such as complexity and length.

Related information

Device passwords, 92

Controlling when devices delete all data in the work space

To protect your organization's data on BlackBerry Balance devices running BlackBerry 10 OS, you can delete all work data from the device by wiping the work space and all of its contents. All personal data remains on the device. For example, you can do this if a user no longer works at your organization.

The following table lists examples of data that is removed when devices delete all data from the work space:

Item	Description
Work email messages	• Email messages that are sent to the user's work email account and email messages that the user sends from the work email account • Draft email messages that the user creates using their work email account
Attachments	• Attachments that are sent to the user's work email account and attachments that the user sends from the work email account • Attachments that the user saves to the work space
Calendar entries	Calendar entries that the user creates using their work calendar
Contacts	Contacts that the BlackBerry Device Service synchronizes with the user's work email account
BlackBerry Remember	All tasks and memos that the BlackBerry Device Service synchronizes with the user's work email account
Browser	All work browser data
Files	Files that the user accessed and downloaded from your organization's network
IT policy	IT policy that is associated with your organization
Device transport key	References to the device transport key, which prevents the device from communicating with the BlackBerry Device Service
Work apps	Work apps that a user downloaded and installed on a device

Item	Description
Work app data	Work data that is associated with work apps on the device
Work Wi-Fi profiles	Work Wi-Fi profiles that the user configures on the device
Work VPN profiles	Work VPN profiles that the user configures on the device

Related information

Data wipe, 99

How the BlackBerry Device Service and devices manage work and personal data and apps

BlackBerry Balance devices running BlackBerry 10 are designed to separate work data from personal data to prevent users from compromising your organization's data on devices. You can also use the BlackBerry Device Service and IT policy rules to manage work and personal data and apps on devices using the following security features:

- Send work space wallpaper to devices
- Control access to work and personal content on devices
- Manage sharing of work and personal files using the Share option
- Manage how apps open links in the work space and the personal space on devices
- Manage work apps using the BlackBerry World for Work storefront
- Manage data transferred to and from devices using NFC
- Manage cloud storage apps in the work space on devices
- Transfer work data from devices using Bluetooth profiles
- Prevent personal apps from accessing work contacts
- Prevent users from sharing work data on devices when sharing the screen during BBM Video chats
- Prevent users from using voice control commands on devices
- Prevent users from using voice dictation within work apps on devices
- Back up and restore work data on devices

Sending work space wallpaper to devices

To help users distinguish between the work space and the personal space on BlackBerry Balance devices running BlackBerry 10, the home screen in each space displays different, visually distinct wallpapers by default. This gives users a strong visual indication of which space they are currently working in.

You can also choose to apply a customized work wallpaper image file for work space wallpaper. After you specify an image file, the Enterprise Management Web Service sends the work space wallpaper to devices in the BlackBerry Device Service domain and users cannot change their work space wallpaper to a different wallpaper image.

When users are in the work space on devices, they see the work space wallpaper. If you do not send a work space wallpaper image to devices, users can still set a different wallpaper image for the work space using the Wallpaper option in the Display settings, from the work space on devices. If a user selects images, such as pictures, as their work space wallpaper, the device saves a copy of the image in case it is deleted or the media card that it is stored on is removed from the device. Users can set the personal space wallpaper using the Wallpaper option in the Display settings on devices, from the personal space on devices.

The work space wallpaper that you send to devices is stored in a protected folder on devices that is separate from the folders that store other wallpaper images and is removed if the work space is removed.

For more information about sending work space wallpaper to devices, see the *BlackBerry Device Service Advanced Administration Guide*.

Controlling app access to work and personal content on devices

Files and data are stored in either the work space or personal space on BlackBerry Balance devices running BlackBerry 10 OS. Devices do not permit users to move files from the personal space to the work space or from the work space to the personal space. Devices do not permit users to cut, copy, or paste text from work space apps to personal space apps. Devices do permit users to cut, copy, or paste text from personal space apps to work space apps. Devices store data that users copy from work space apps in the work space only and data that users copy from personal space apps in the personal space only. Apps that are available in the work and personal spaces in a unified view can attach personal files to the work portion of the app. For example, users can attach personal files to work email messages. Devices use read-only versions of these files and do not transfer or copy those files from the personal file system to the work file system.

By default, work apps can access shared files that are located in the personal space if a user permits it. When a user installs a work app, the device displays a message that provides the user with the option to allow or deny the app's request to access shared files. If you want to prevent work apps from accessing shared personal files, set the "Work App Access to Shared Files in the Personal Space" IT policy rule to Disallow. This will prevent work apps from accessing shared personal files regardless of the user settings on the device and users cannot attach personal files to messages sent from a work account.

By default, all apps in the personal space can access required data for work contacts.

You can change IT policy rule settings to:

- Prevent all personal apps from accessing data for work contacts all the time by setting the "Personal Apps Access to Work Contacts" IT policy rule to None
- Allow only the following personal apps developed by RIM to access data for work contacts by setting the "Personal Apps Access to Work Contacts" IT policy rule to Only RIM Applications: Phone, BlackBerry Messenger (including BBM Video and BBM Voice), Text Messages, Smart Tags, visual voice mail, and voice dialing.

Managing sharing of work and personal files using the Share option on devices

BlackBerry Balance devices running BlackBerry 10 allow users to share personal files with work apps using the Share option. If users want to share personal files with work apps, the work space must be unlocked.

Users can share work files only with work apps using the Share option.

You can prevent users from sharing work content using Bluetooth or NFC by setting the "Transfer Work Files Using Bluetooth OPP" IT policy rule to Disallow.

Related information

Transferring work data from devices using Bluetooth, 55

Managing how apps open links in the work and personal spaces on devices

In general, work apps can open only other work apps and personal apps can open only other personal apps on BlackBerry Balance devices running BlackBerry 10. For example, if users click on links in personal email messages, the browser in the personal space will open. There are a few cases where work apps will open apps that are classified as personal apps, such as Phone, BBM, or SMS. In these cases, devices have restrictions in place to protect against data leakage and to ensure that only the minimum amount of data required to initiate the personal apps is passed between the work apps and the personal apps.

By default, users can use the browser in the personal space to open links in both personal and work email messages. Links in work email messages will open in the browser in the personal space and devices display a message that provides users with the option to open the link in the browser in the work space instead.

Your organization may require that intranet links be opened in the browser in the work space. If you want to prevent users from using the browser in the personal space to open links in work email messages, you can set the "Open Links in Work Email Messages in the Personal Browser" IT policy rule to Disallow and links in work email messages will always open the browser in the work space.

Managing work apps using the BlackBerry World for Work storefront

After BlackBerry 10 devices are activated on the BlackBerry Device Service using the BlackBerry Balance option, devices have two separate BlackBerry World storefront clients: BlackBerry World located in the personal space and BlackBerry World for Work located in the work space.

BlackBerry World for Work contains a Company Apps tab and a Public Apps tab. The Company Apps tab provides a list of apps that are hosted by your organization and that you have specified as optional apps. The Public Apps tab provides a list of apps that are available from the public BlackBerry World storefront that you have specified as optional apps.

Users can install only apps that are hosted by your organization that you deploy using the BlackBerry Device Service and public BlackBerry World apps that you specify as optional apps in the work space on devices. Users cannot choose to install apps that have not been approved by your organization in the work space on devices. All apps that users download from the public BlackBerry World are installed in the personal space on devices.

If any of the apps that you specify as optional apps that users can install in the work space do not meet specific criteria for devices (for example, service provider, country, or device version), the apps will not appear in the BlackBerry World for Work storefront on those devices.

Devices classify Android apps as personal apps and you cannot specify Android apps as optional apps that users can install in the work space.

For more information about specifying apps in the BlackBerry World for Work storefront on devices in your organization, see the *BlackBerry Device Service Advanced Administration Guide*.

Related information

Managing app availability on devices, 83
BlackBerry World for Work, 78

Managing data transferred to and from a device using NFC

Data that a BlackBerry Balance device running BlackBerry 10 receives from another device using NFC is generally classified as personal data. However, if a work app supports a specific NFC tag format that is unique to the work app, any data that the device receives with that NFC tag is classified as work data.

By default, devices can use NFC to send work data to other NFC-enabled devices. You can prevent users from sharing work data in a file format (for example, pictures or documents) using NFC by setting the "Transfer Work Files Using Bluetooth OPP" IT policy rule to Disallow. Regardless of how this IT policy rule is set, devices can use NFC to send certain MIME or URI data types, such as web addresses and phone numbers to other NFC-enabled devices.

Managing cloud storage apps in the work space on devices

BlackBerry Balance devices running BlackBerry 10 support cloud storage apps in both the work space and the personal space on devices. By default, users can use cloud storage apps developed by Research In Motion, such as Box and Dropbox, in the work space on devices. After users log into a cloud storage app in the work space on devices, that cloud file storage is available as a storage option in the work space and the cloud storage app stores its settings and data in the work space file system. Users can then read, write, move, and update data to that location.

You can prevent cloud storage apps from being available in the work space on devices by setting the "Cloud Storage Access from Work Space" IT policy rule to Disallow so that users can then use these apps only in the personal space on devices.

Transferring work data from devices using Bluetooth

Using Bluetooth wireless technology, users can open wireless connections between a BlackBerry Balance device running BlackBerry 10 OS and other Bluetooth enabled devices. Users must request a pairing with another Bluetooth device and use a passkey to complete the pairing. BlackBerry 10 devices prompt users each time another Bluetooth enabled device tries to connect to their devices.

By default, users can transfer files, contacts, and messages from the work space on BlackBerry 10 devices to Bluetooth enabled devices that they have successfully paired with.

You can use the following IT policy rules to prevent users from transferring work data to other Bluetooth enabled devices:

- Transfer Work Files Using Bluetooth OPP
- Transfer Work Contacts Using Bluetooth PBAP and HFP
- Transfer Work Messages Using Bluetooth MAP

Devices use the Bluetooth OPP to send objects to another Bluetooth enabled device. To prevent a user from using the Bluetooth OPP to send work files and objects such as contacts to another Bluetooth enabled device, you can set the "Transfer Work Files Using Bluetooth OPP" IT policy rule to Disallow. Devices also use the Bluetooth OPP to share work data in a file format (for example, pictures or documents) using NFC. When the "Transfer Work Files Using Bluetooth OPP" IT policy rule is set to Disallow, users cannot share work data in a file format using NFC.

Devices use the Bluetooth PBAP and the Bluetooth HFP to send contacts to another Bluetooth enabled device. To prevent a user from using the Bluetooth PBAP and the Bluetooth HFP to send work contacts to another Bluetooth enabled device, you can set the "Transfer Work Contacts Using Bluetooth PBAP or HFP" IT policy rule to Disallow. If you set this rule to Disallow, devices also cannot use the Bluetooth MAP to send work messages to another Bluetooth enabled device.

Devices use the Bluetooth MAP to send messages to another Bluetooth enabled device. To prevent a user from using the Bluetooth MAP to send messages from the work space (for example, email messages and instant messages) to another Bluetooth enabled device, you can set the "Transfer Work Messages Using Bluetooth MAP" IT policy rule to Disallow. If you set the "Transfer Work Contacts Using Bluetooth PBAP or HFP" IT policy rule to Disallow, users cannot send work messages to another Bluetooth enabled device using the Bluetooth MAP, regardless of what the "Transfer Work Messages Using Bluetooth MAP" IT policy rule is set to.

By default, if the "Transfer Work Messages Using Bluetooth MAP" IT policy rule is set to Allow, a user can transfer work messages to a Bluetooth enabled device using the Bluetooth MAP following a single password prompt to enter the work space. If you want to require a user to unlock the work space each time the device connects to the Bluetooth enabled device before the device can transfer work messages using the Bluetooth MAP, you can set the "Transfer Work Messages Using Bluetooth MAP Without Prompt" IT policy rule to Disallow.

Preventing users from sharing work data on devices when sharing the screen during BBM Video chats

By default, users can share the screen with other BBM Video chat participants during a BBM Video chat when they are in the work space on BlackBerry Balance devices running BlackBerry 10.

If you want to prevent users from sharing work screens with other BBM Video chat participants when users share the screen during a BBM Video chat, you can set the "Share Work Data During BBM Video Screen Sharing" IT policy rule to Disallow. If you set this rule to Disallow, a device locks the work space when a user shares the screen during a BBM Video chat and the user cannot unlock the work space until the screen sharing part of the BBM Video chat is complete.

Controlling voice control

By default, users can use voice control commands on BlackBerry 10 devices. To prevent users from using voice control commands for Email and Calendar apps on devices, set the "Voice Control" IT policy rule to Disallow for Email and Calendar. To prevent users from using any voice commands on devices, set this rule to Disallow.

For more information, visit blackberry.com/go/kbhelp to read article KB33430.

Preventing users from using voice dictation within work apps on devices

By default, users can use voice dictation in all apps that support this feature on BlackBerry Balance devices running BlackBerry 10.

If you want to prevent users from using voice dictation in work apps, you can set the "Voice Dictation in Work Apps" IT policy rule to Disallow.

Backing up and restoring work data on devices

By default, users can back up and restore both work data and personal data that is stored on BlackBerry Balance devices running BlackBerry 10 using BlackBerry Link. Users can restore the backed up data to devices after the device software is updated or if issues occur that require users to restore the information. Users can restore the data to the same device or transfer it to another device. The data is encrypted and stored on the users' computers.

If you want to prevent users from backing up and restoring apps and data that are located in the work space on devices, you can set the "Backup and Restore Work Space" IT policy rule to Disallow. When you set this rule to Disallow, the option to back up and restore the contents of the work space is disabled in BlackBerry Link.

Related information

Back up and restore, 101

Controlling how work and personal apps connect to your organization's network

The BlackBerry Device Service controls how work apps and personal apps on BlackBerry Balance devices running BlackBerry 10 connect to your organization's network. Work data traffic and personal data traffic are routed independently, and you can use IT policy rules to control the type of connections that work data and personal data use to connect to your organization's network. Apps that are in the work space on devices can access and connect only to your organization's network and cannot connect to personal networks. By default, personal apps can access and connect to personal networks and your organization's network.

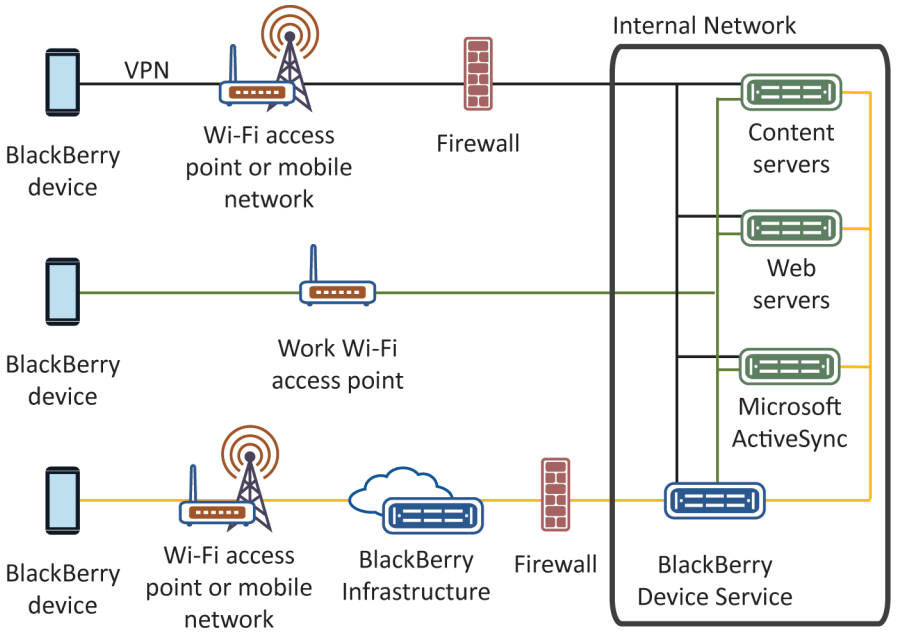
Work apps and personal apps can access your organization's network using a number of communication methods. Based on the settings of IT policy rules, certain interfaces are available to apps that are in the work space and the personal space on devices. Those interfaces are prioritized and apps usually use the default route for the space that they are located in.

The "Network Access Control for Work Apps" and "Work Data Uses Only Work Network" IT policy rules control what interfaces are available to apps that are in the work space. The "Network Access Control for Work Apps" IT policy rule controls whether work apps on a device must connect to your organization's network through the BlackBerry Device Service. The "Work Data Uses Only Work Network" IT policy rule controls whether a device must route work traffic through a work VPN or work Wi-Fi connection and cannot go through the BlackBerry Infrastructure.

The "Network Access Control for Work Apps" IT policy rule controls what interfaces are available to work apps. If the "Network Access Control for Work Apps" IT policy rule is set to No, work apps attempt to connect to your organization's network using the following communication methods, in order:

1. Work VPN profiles over a Wi-Fi network
2. Work VPN profiles over a mobile network
3. Work Wi-Fi profiles
4. BlackBerry Infrastructure over a Wi-Fi network
5. BlackBerry Infrastructure over a mobile network

However if the "Work Data Uses Only Work Network" IT policy rule is set to Yes, the #4 and #5 communication methods above are not available.

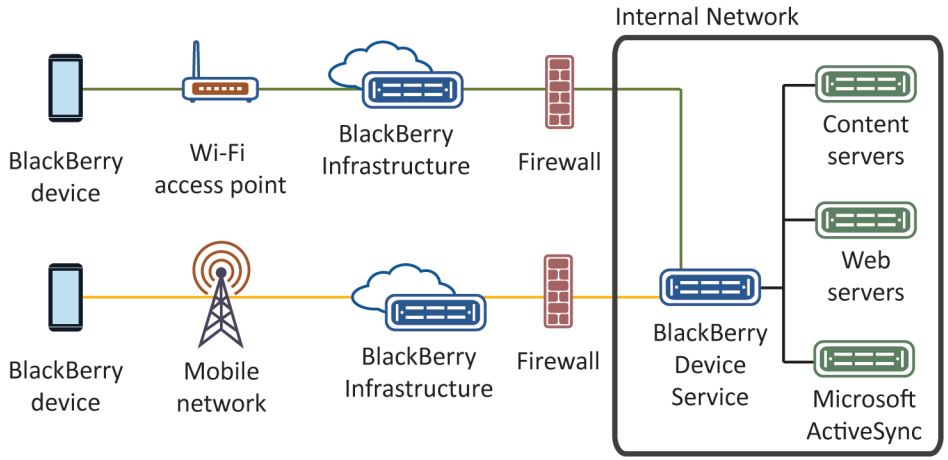


By default, work apps can use the Wi-Fi profiles or VPN profiles that are stored on the device to connect to your organization's network and can also connect to your organization's network through the BlackBerry Device Service. If you want to control or filter all work traffic on devices, you can set the "Network Access Control for Work Applications" IT policy rule to Yes. When you set this rule to Yes, you disable Wi-Fi and VPN connections for work apps and limit connectivity exclusively to the BlackBerry Device Service (BlackBerry MDS Connection Service and the BlackBerry Infrastructure).

If the "Network Access Control for Work Apps" IT policy rule is set to Yes, work apps attempt to connect to your organization's network using the following communication methods, in order:

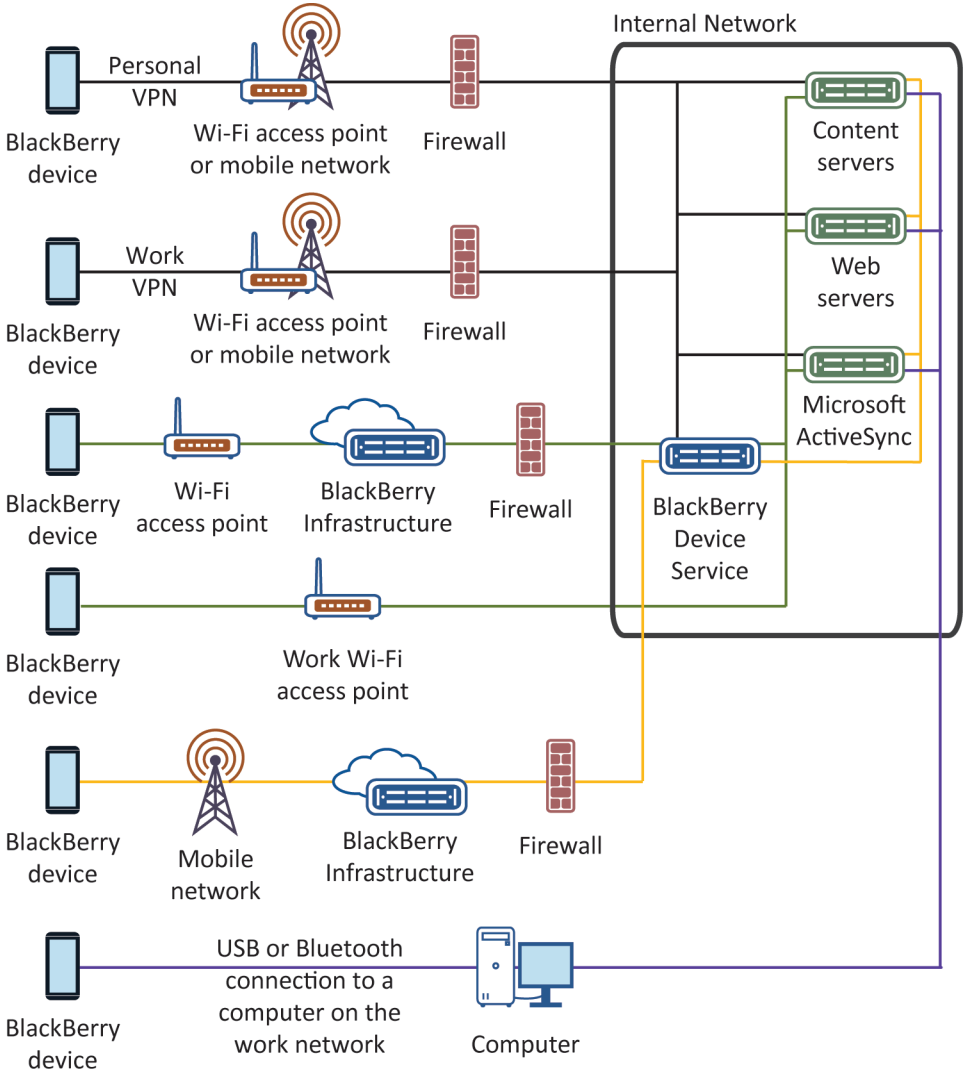
1. BlackBerry Infrastructure over a Wi-Fi network
2. BlackBerry Infrastructure over a mobile network

In this case, also setting the "Work Data Uses Only Work Network" IT policy rule to Yes will not allow any communication methods and therefore it is not recommended that you set both of these rules to Yes.



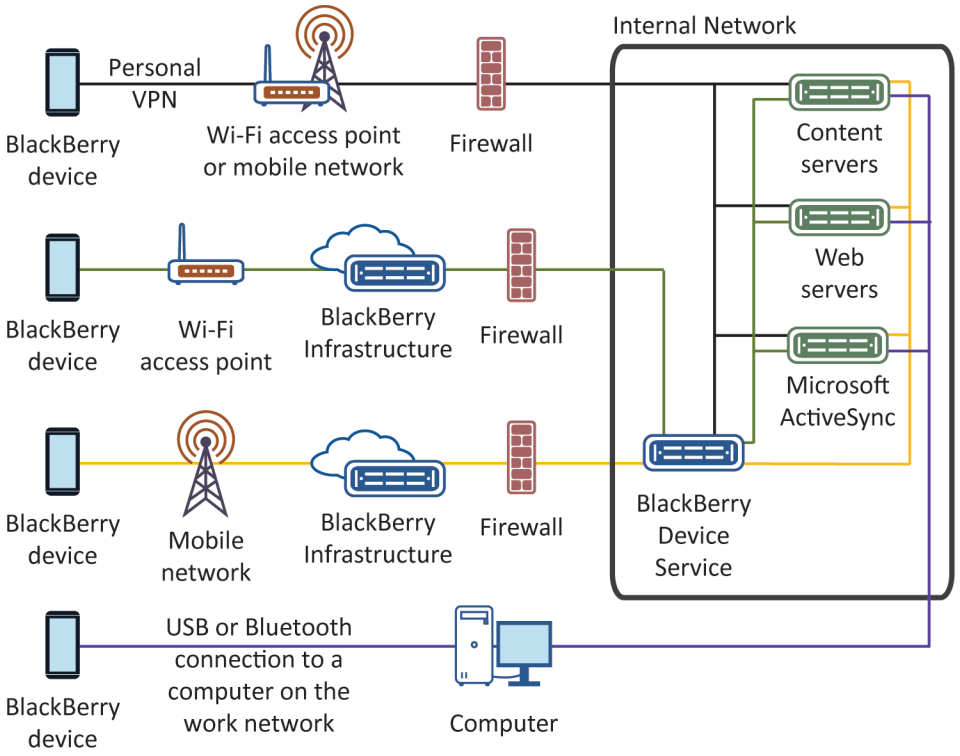
The "Work Network Usage for Personal Apps" IT policy rule controls what interfaces are available to apps that are in the personal space. If the "Work Network Usage for Personal Apps" IT policy rule is set to Allow, personal apps attempt to connect to your organization's network using the following communication methods, in order:

1. Personal VPN profiles over a Wi-Fi network
2. Personal VPN profiles over a mobile network
3. Work VPN profiles over a Wi-Fi network
4. Work VPN profiles over a mobile network
5. Personal Wi-Fi profiles
6. Work Wi-Fi profiles
7. Mobile network
8. Tethered to another device using USB or Bluetooth connections



If the "Work Network Usage for Personal Apps" IT policy rule is set to Disallow, personal apps attempt to connect to your organization's network using the following communication methods, in order:

1. Personal VPN profiles over a Wi-Fi network
2. Personal VPN profiles over a mobile network
3. Personal Wi-Fi profiles
4. Mobile network
5. Tethered to a computer or another device using USB or Bluetooth connections



You can use IT policy rules to prevent or protect connections to your organization's network:

- Prevent personal apps from using your organization's networks to connect to the Internet
- Allow the BBM Video feature to use your organization's networks when personal apps cannot

For more information about IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Preventing personal apps on devices from using your organization's networks to connect to the Internet

By default, all apps in the personal space on BlackBerry Balance devices running BlackBerry 10 can use your organization's Wi-Fi or VPN network to connect to the Internet.

If you want to prevent all apps in the personal space from using your organization's networks to connect to the Internet, you can set the "Work Network Usage for Personal Apps" IT policy rule to Disallow. If you prevent all personal apps from using your organization's networks to connect to the Internet and if a personal network is not available, personal apps that need access to the Internet might not work.

If the "Work Network Usage for Personal Apps" IT policy rule is set to Allow, users can still prevent all apps in the personal space from using your organization's network to connect to the Internet using the Allow Personal Apps to Use Work Networks option in the BlackBerry Balance settings on the device. Users may choose to do this in order to protect their privacy.

Preventing the BBM Video feature on devices from using your organization's networks

The BBM Video feature is classified as a personal app on BlackBerry Balance devices running BlackBerry 10. By default, if the "Work Network Usage for Personal Apps" IT policy rule is set to Allow, the BBM Video feature on devices can use your organization's Wi-Fi network, VPN network, or the BlackBerry MDS Connection Service for incoming and outgoing video chats.

However, even if you allow personal apps to use your organization's networks to connect to the Internet (by setting the "Work Network Usage for Personal Apps" IT policy rule to Allow), you can prevent the BBM Video feature from using your organization's networks by setting the "BBM Video Access to Work Network" IT policy rule to Disallow.

8 Using BlackBerry Balance to secure BlackBerry PlayBook tablets in your organization's environment for work use

Your organization can use BlackBerry Balance technology to permit users to use BlackBerry PlayBook tablets for both work and personal use. For example, your organization might want to permit users to activate their personal devices on the BlackBerry Device Service or permit users to use devices that your organization provides for personal use.

The BlackBerry Device Service permits you to manage the work file system on tablets that run BlackBerry PlayBook OS 2.0 or later. Security features on tablets can control how the tablet helps protect your organization's data and applications.

The BlackBerry Device Service security features allow you to:

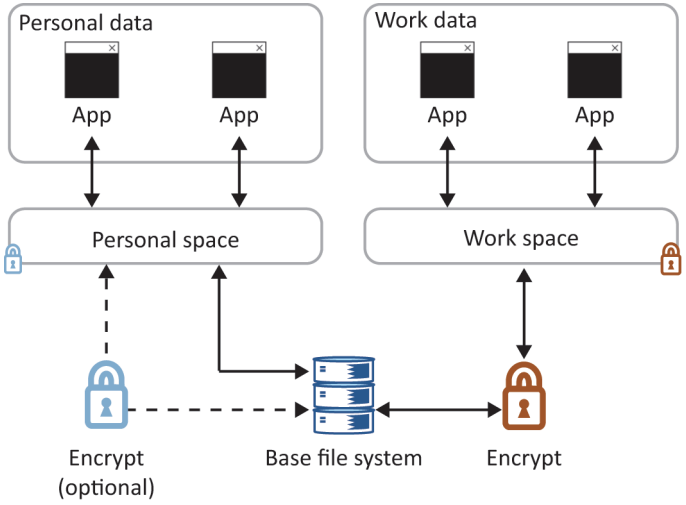
- Control the connections that tablets make to your organization's environment, including connections to your work Wi-Fi networks and Microsoft ActiveSync
- Install and manage your organization's applications on tablets
- Protect your organization's data and applications on tablets

How BlackBerry PlayBook tablets distinguish between work data and personal data

Work data consists of IT policies, profiles, and software configurations that the BlackBerry Device Service and BlackBerry PlayBook tablets send to each other, data (such as email messages, calendar entries, and attachments) that tablets receive from your organization's network using connections with the BlackBerry Device Service.

To help protect work data, tablets automatically create a work space in the BlackBerry PlayBook OS during the activation process that isolates work data and work apps from personal data and personal apps. Tablets encrypt the work file system using XTS-AES-256 encryption.

Tablets encrypt data stored in the personal file system if you set the "Personal Space Data Encryption" IT policy rule to Yes or if the user turns on encryption for personal data using the Encryption option in the Security settings on tablets. Tablets encrypt data stored in the personal file system using XTS-AES-256 encryption.



How BlackBerry PlayBook tablets protect work data

BlackBerry PlayBook tablets are designed to encrypt data stored in the work file system using XTS-AES-256.

Tablets use a randomly generated 512-bit file encryption key to encrypt the contents of a file. The file encryption process creates a security record for the encrypted file that consists of a 512-bit random salt, the file encryption key, and several attributes of the file. Tablets encrypt the file security record using the domain key, which is a 512-bit randomly generated key.

Tablets use the domain key to encrypt all file security records in the work file system. The domain key is stored in a security record that is similar to the file security record. The domain security record is encrypted using the work space key. The work space key is stored in RAM and is not written to persistent storage on the tablet.

The tablet system key and the domain key are stored in NVRAM on tablets and are encrypted with a key that is stored in the replay protected memory block in flash memory. The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured.

Tablets can also encrypt the data stored in the personal file system if you set the "Personal Space Data Encryption" IT policy rule to Yes or if users turn on encryption for personal data using the Encryption option in the Security settings on tablets.

Related information

How a BlackBerry PlayBook tablet protects personal data, 67

Data flow: Generating a work space key when the "Two-factor Encryption Key Generation" IT policy rule is set to Yes

If you set the "Two-factor Encryption Key Generation" IT policy rule to Yes, BlackBerry PlayBook tablets base the encryption key on both the protected secret and the password for the work space. For more information about IT policies, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

1. The user types the password for the work space to unlock the work space.
2. The tablet performs the following actions:
   a Uses the password, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive an intermediate key.
   b Uses SHA-512 to hash the intermediate key and the tablet system key to produce the work space key.

   The tablet system key is created during the manufacturing process and is the SHA-512 hash of a hardware ID and a 512-bit random key.

   c Overwrites and then frees the memory that stored the password, the intermediate key, and the work space key when it is finished using them.

Data flow: Generating a work space key when the "Two-factor Encryption Key Generation" IT policy rule is set to No

If you set the "Two-factor Encryption Key Generation" IT policy rule to No, BlackBerry PlayBook tablets base the encryption key on the protected secret only. For more information about IT policies, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

To generate a work space key, tablets perform the following actions:

1. Retrieves the domain key from the NV store on the tablet.
2. Uses the domain key, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive an intermediate key.
3. Uses SHA-512 to hash the intermediate key and the tablet system key to produce the work space key.

   The tablet system key is created during the manufacturing process and is the SHA-512 hash of a hardware ID and a 512-bit random key.

4. Overwrites and then frees the memory that stored the domain key, the intermediate key, and the work space key when it is finished using them.

Controlling when BlackBerry PlayBook tablets delete all data in the work space

To protect your organization's data on a BlackBerry PlayBook tablet, you can delete all work data from the tablet by wiping the work space and all of its contents. All personal data remains on the device. For example, you can do this if a user no longer works at your organization.

Users can remove the work space from their tablets using the delete option in the BlackBerry Balance settings on the tablet.

To require that a tablet delete all data in the work space, you can use the BlackBerry Device Service to send the "Delete only the organization data and remove device" IT administration command to the tablet. If the BlackBerry Device Service cannot connect to the tablet because the tablet is turned off or not connected to a network, the BlackBerry Device Service sends the command after the tablet connects to a network. A user can still use the tablet while the tablet deletes the data in the work space. For more information about sending the "Delete only the organization data and remove device" IT administration command to tablets, see the *BlackBerry Device Service Advanced Administration Guide*.

You can also use the "Wipe the Work Space without Connectivity" and "Maximum Password Attempts" IT policy rules to require that a tablet deletes the work space under specific conditions.

You can set the "Wipe the Work Space without Network Connectivity" IT policy rule to the number of hours that must elapse when a tablet does not connect to your organization's network before the tablet deletes all data in the work space. You can use this rule to make the tablet delete the data in the work space if the tablet cannot receive updates or commands from the BlackBerry Device Service.

You can set the "Maximum Password Attempts" IT policy rule to the number of times that a user can try an incorrect password on a tablet before the tablet deletes all data in the work space.

The following table lists examples of the data that is removed when tablets delete all data from the work space:

Item	Description
Work email messages	• Email messages that are sent to the user's work email account and email messages that the user sends from the work email account • Draft email messages that the user creates using their work email account
Attachments	Attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
Calendar entries	Calendar entries that the user creates using their work calendar
Contacts	Contacts that the BlackBerry Device Service synchronizes with the user's work email account
Browser cache	Browser cache, Bookmarks, History, and Cookies.
Files	Files that the user accessed and downloaded from your organization's network

Item	Description
IT policy	IT policy that is associated with your organization
Device transport key	References to the device transport key, which prevents the tablet from communicating with the BlackBerry Device Service
Work data	Work data that is associated with work apps on the tablet
Wi-Fi and VPN profiles	Wi-Fi and VPN profiles that the user configures on the tablet

You can also use the BlackBerry Device Service service to send the "Delete all device data and remove device" IT administration command to the tablet to delete all data from the entire tablet. For more information about sending the "Delete all data and remove device" IT administration command to devices, see the *BlackBerry Device Service Advanced Administration Guide*.

Deleting all data from the work space on a BlackBerry PlayBook tablet

When you or a user deletes all data from the work space on a BlackBerry PlayBook tablet, the BlackBerry PlayBook OS instructs the file system to delete all directories and files in the work file system.

Any files that persist in the work file system remain encrypted. The decryption key is not accessible to the file system.

How a BlackBerry PlayBook tablet protects personal data

The BlackBerry PlayBook tablet allows the encryption of personal data on the tablet.

You can use the "Personal Space Data Encryption" IT policy rule to turn on encryption for the personal space of a tablet. If this rule is set to Yes, the personal space of the tablet is encrypted. If this rule is set to No, users can choose to encrypt the personal space using the Encryption option in the Security settings on the tablet.

If encryption is turned on for the personal space of the tablet, the tablet encrypts data that is stored in the personal file system using XTS-AES-256 encryption. Each file in the personal file system is encrypted with a randomly generated key. The keys are then encrypted by a series of encryption keys that chain to a key that is embedded in the processor when the processor is manufactured.

If you set the "Personal Space Data Encryption" IT policy rule to Yes, you should also set the "Apply Work Space Password to Full Device" IT policy rule to Yes so that the password applies to the entire tablet. If you set the "Personal Space Data Encryption" IT policy rule to No and the user chooses to encrypt personal data, the tablet prompts the user to enter a new password if the tablet does not already have a password.

Related information

Device passwords, 92
How BlackBerry PlayBook tablets protect work data, 64

What happens when a user updates or creates files on a BlackBerry PlayBook tablet

The BlackBerry PlayBook tablet helps protect data when a user performs the following actions:

Action	Description
Open a file to view or update it	When the user opens a file that belongs to one space, the tablet starts the app in the space mode that the file belongs to. For example, if the user opens a work file, the tablet starts the File Manager app in work mode.
Copy and paste data to a file	The tablet does not permit the user to move data from the work space to the personal space. For example, the user cannot cut, copy, or paste data from a work file to a personal file. The tablet does permit a user to move data from the personal space to the work space. For example, the user can cut, copy, or paste personal data into a work file. The user can also attach a personal file to a work email message or work calendar entry.

How a BlackBerry PlayBook tablet controls whether an app is a work or personal app

Apps on a BlackBerry PlayBook tablet can run in work mode or personal mode. By default, all apps on a tablet run in personal mode.

When you use the BlackBerry Device Service to install and manage apps on tablets, the apps are considered work apps. The tablet automatically installs required apps in the work space after the tablet downloads them. A user can download and install optional apps from the Work tab in the BlackBerry World storefront. The required and optional apps are installed in the work space on tablets. Work apps can only access work data and interact with other work apps that are also located in the work space.

The work apps have read-only access to the personal apps and personal data that are located in the personal space.

Some apps, such as Documents To Go, can run in work mode or personal mode. If the user opens an attachment in a work email message or work calendar entry, Documents To Go runs in work mode. If the user opens an attachment in a personal email message or personal calendar entry, Documents To Go runs in personal mode.

Determining which apps are work or personal apps

The following table lists the apps that a BlackBerry PlayBook tablet permits to run in work mode or personal mode.

App	Work mode	Personal mode
Apps that a user downloads and installs on the tablet		√
Apps that a user downloads from the Work tab on the BlackBerry World storefront (the apps that you specified as optional)	√	
Apps that are sent to the tablet using software configurations in the BlackBerry Device Service	√	
Browser	√	√
Calendar	√	√
Contacts	√	√
Document viewers (for example, Documents To Go and Adobe Reader)	√	√
File Manager	√	√
Messages	√	√
Music	√	√
Pictures	√	√
Print To Go	√	√
Videos	√	√
Work Browser	√	

Comparison of work and personal apps

Work apps	Personal apps
Work apps can view and change work data. Work apps can view but not change personal data.	Personal apps cannot view work data but they can view and change personal data.
Work apps can attach personal files to work email messages or work calendar entries (for example, a tablet user can attach a picture that the user took using the tablet camera to a work email message).	Personal apps cannot attach work files to personal email messages or personal calendar entries.
A user can access work apps when you activate a tablet on the BlackBerry Device Service.	A user can access personal apps regardless of whether you are using the BlackBerry Device Service to manage work apps on the tablet
The tablet upgrades work apps when the BlackBerry PlayBook OS is upgraded.	The tablet upgrades preinstalled personal apps when the BlackBerry PlayBook OS is upgraded. The user can upgrade the personal apps that the user installs at any time.

Access rights for work and personal data that the BlackBerry PlayBook OS grants to apps

The following table displays the access rights that apps on BlackBerry PlayBook devices have to work data or personal data.

Access right	Work app A	Work app B	Personal app C	Personal app D
Access a work file that a work app saves	Read-write access	Read-write access	No access	No access
Access a personal file that a personal app saves	Read-only	Read-only	Read-write access	Read-write access
Access the private data of Work app A	Read-write access	No access	No access	No access
Access the private data of Personal app C	No access	No access	Read-write access	No access

How a BlackBerry PlayBook tablet is designed to prevent BlackBerry Runtime for Android apps from accessing work data or apps

Tablets consider Android apps to be personal apps and install them in the personal spaces on BlackBerry PlayBook tablets. Android apps can only access personal data that is located in the personal space. Android apps do not have access to the work apps and work data that are located in the work space.

You cannot add Android apps to the Work tab of the BlackBerry World storefront on the tablet. If you specify an Android app from BlackBerry World as an optional app, it does not appear on the Work tab of BlackBerry World on the tablet and users cannot install it in the work space.

You cannot manage or remove the Android apps that users install on their tablets.

Controlling the network connections that work and personal apps on BlackBerry PlayBook tablets can access

The BlackBerry Device Service controls how work apps and personal apps on BlackBerry PlayBook tablets can connect to your organization's network.

Both work apps and personal apps can use the Wi-Fi profiles or VPN profiles that are stored on the tablet to connect to your organization's network.

Work apps can also connect to your organization's network through the BlackBerry Device Service. You can use the "Network Access Control for Work Apps" IT policy rule to disable Wi-Fi and VPN connections for work apps and limit connectivity to the BlackBerry MDS Connection Service and the BlackBerry Infrastructure.

Using the browser to connect a BlackBerry PlayBook tablet to web servers that support NTLM

NTLM is a suite of security protocols that Microsoft designed to provide authentication, integrity, and confidentiality for web connections.

If a user uses the browser to connect to web servers that support NTLM using a work Wi-Fi network or a work VPN network, the tablet supports NTLMv1 authentication. The tablet also supports the message-signing capabilities of both NTLMv1 standard session security and NTLM Extended Session Security (also known as NTLM2). The web servers can be located either inside or outside of your organization's environment.

How work apps are installed on a BlackBerry PlayBook tablet

If you configure required and optional apps for BlackBerry PlayBook tablets using the BlackBerry Device Service, the BlackBerry Device Service adds the apps to a shared network folder for apps that you specified. If you configure an app that is publicly available in the BlackBerry World storefront as an optional app, it is not added to the shared network folder for apps.

Apps that you specify as required are installed on the tablet. Users can install apps that you specify as optional from the Work tab of BlackBerry World on the tablet. The optional apps that are in the shared network folder are sent to the tablets from your organization's network. They are not uploaded to the BlackBerry World servers and are not available to users who are outside of your organization.

For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

Related information

Managing app availability on devices, 83

When a BlackBerry PlayBook tablet prevents a user from accessing work data or apps

You can use the BlackBerry Device Service to allow a user to access work data and work apps on a BlackBerry PlayBook tablet. A tablet does not permit the user to access work data or work apps when you or the user deletes all tablet data.

If you configure the "Password Required for Work Space" IT policy rule to enforce the use of a password for the work space and the user types the password for the work space incorrectly more than the "Maximum Password Attempts" IT policy rule permits, the tablet closes all work apps and deletes the work space.

Personal data and personal apps are not affected by the actions that the tablet performs to prevent the user from accessing work data and work apps.

Securing work space only devices

9

You can activate devices using the work space only option. These devices contain only one space that is considered a work space and is secure. All data and apps on these devices are classified as work resources. You can activate work space only devices if users will use devices almost exclusively for work purposes or if you have particularly sensitive positions in your organization that require full management of the devices.

With this activation option, you have full control over devices and you can:

- Approve all apps and services on devices
- Log communication paths for phone calls or SMS messages
- Disable device features such as the camera or GPS
- Block communication paths such as Wi-Fi or Bluetooth
- Control what apps users can download
- Prevent access to personal email messaging services

Password protection on work space only devices is not optional. To secure work data on these devices, users must set a device password during activation.

Users with work space only devices should be aware that your organization can audit all data on their devices, even if they are using their devices for personal use. When a device is activated using the work space only option, the user is presented with a general disclaimer stating that the device is completely managed by your organization and the user must accept the disclaimer for activation to continue. You can configure an additional notice that outlines the terms and conditions that users must follow to comply with your organization's security requirements.

To use this activation option, devices must be running BlackBerry 10 OS version 10.1 or later on BlackBerry Enterprise Service 10. If a device has a personal space or a work space before you activate it, it is wiped during the activation process and any data, apps, or network connections that the device used before activation are removed. For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

Securing data

Security features on BlackBerry Enterprise Service 10 and work space only devices classify, protect, and manage work data and work apps.

Classifying data

All data and apps on work space only devices are classified as work resources, even when users use the devices for personal tasks like visiting personal web pages or receiving personal email messages.

Protecting data

Work space only devices protect work data by encrypting the files stored in the work space. Devices can also encrypt the files stored on media cards. Only the contents of files are encrypted; the files themselves or directory names are not encrypted.

You can protect data further by controlling device password requirements and controlling when device wipes occur.

Related information

Protecting data, 92

Work space encryption

Work space only devices encrypt data stored on devices using XTS-AES-256.

A device randomly generates an encryption key to encrypt the contents of a file. The file encryption keys are protected by a hierarchical system of encryption keys as follows:

- The device encrypts the file encryption key with the work domain key and stores the encrypted file encryption key as a metadata attribute of the file.
- The work domain key is a randomly generated key that is stored in the file system metadata and is encrypted using the work master key.
- The work master key is also randomly generated. The work master key is stored in NVRAM on the device and is encrypted with the system master key.
- The system master key is stored in the replay protected memory block on the device.
- The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured.

These keys are generated using the BlackBerry OS Cryptographic Kernel, which is FIPS 140-2 certified.

Media card encryption

By default, work space only devices allow users to save data to media cards, and that data is stored in an unencrypted format.

Because users can store work data on media cards in an unencrypted format by default, it is highly recommended that you turn on media card encryption using the "Media Card Encryption" IT policy rule.

To prevent users from saving data to media cards, you can set the "Media Card" IT policy rule to Disallow.

Related information

Media cards, 103

Password protection

Password protection on work space only devices is not optional. To secure work data on these devices, users must set a device password during activation.

You can use IT policy rules to control device password requirements such as complexity and length.

Related information

Device passwords, 92

Remote wipe

To protect your organization's data on work space only devices, you can wipe a device remotely if, for example, a user no longer works at your organization.

Because these devices only have a work space, you can use either the "Delete all device data and remove device" or "Delete only the organization data and remove device" IT administration commands in the BlackBerry Device Service to wipe these devices.

Related information

Data wipe, 99

Managing data

You can use security features and set IT policy rules to manage work space only devices.

Using the BlackBerry Device Service, you can control the following:

- Connections
- Messaging
- Logging
- Apps
- Access
- Features
- Software
- Wallpaper

Controlling connections

By default, work space only devices can make various network connections. You can use the following IT policy rules to control connections:

- Bluetooth

- Hotspot Browser
- NFC
- User-Created VPN Profiles
- Wi-Fi

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Related information

Controlling Bluetooth, 76

Controlling Bluetooth

Bluetooth wireless technology lets users open wireless connections with other Bluetooth enabled devices. A user must request a pairing with the other device and use a passkey to complete the pairing. Users are prompted every time a new device tries to connect to their device.

By default, work space only devices can use Bluetooth. You can prevent a device from using Bluetooth by setting the "Bluetooth" IT policy rule to Disallow. If you allow Bluetooth on a device, the user can still turn off Bluetooth using device settings.

If a device has Bluetooth turned on, it can use Bluetooth Discoverable Mode. A device that is discoverable can be found by other Bluetooth enabled devices within range of the device. You can prevent a device from using Bluetooth Discoverable Mode by setting the "Bluetooth Discoverable Mode" IT policy rule to Disallow. If you allow Discoverable Mode on a device, the user can still turn it off using device settings.

If a device has Bluetooth and Discoverable Mode turned on, you can prevent a device from opening new connections with other devices by setting the "Bluetooth Pairing" IT policy to Disallow. After a work space only device has connected to other devices, you can use this rule to prevent it from connecting to additional devices.

You can also control some of the criteria that a device must use when it pairs with another device such as passkey length, encryption key length, and pairing method.

By default, a device can connect to another device if the passkey that the other device requests or provides is less than 8 digits. To prevent a device from accepting short passkeys, you can set the "Enforce Minimum Bluetooth Passkey Length" IT policy rule to Yes.

By default, a device must use a minimum encryption key length of 1 byte to encrypt Bluetooth connections. You can use the "Minimum Bluetooth Encryption Key Length" IT policy rule to change the minimum encryption key length.

When devices use Bluetooth Secure Simple Pairing to connect to another device that is running Bluetooth version 2.1 or later, you can require that devices use the numeric comparison mode to connect by setting the "Enforce Bluetooth Secure Simple Pairing Numeric Comparison" IT policy rule to Yes. By default, devices aren't required to use numeric comparison mode.

Devices use Bluetooth profiles to communicate with other Bluetooth enabled devices and carry out tasks such as streaming audio files to another device or allowing another device to access certain types of data. If the "Bluetooth" IT policy rule is set to Allow and Bluetooth is turned on, you can use the following IT policy rules to make all or some Bluetooth profiles unavailable:

- Bluetooth A2DP
- Bluetooth AVRCP
- Bluetooth Contacts Transfer Using PBAP

- Bluetooth File Transfer Using OBEX
- Bluetooth HFP
- Bluetooth MAP
- Bluetooth PAN
- Bluetooth SPP

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Controlling messaging

By default, users can set up various messaging methods on work space only devices such as Facebook and text messaging. You can use the following IT policy rules to control what types of messaging users can do on their devices:

- BBM
- BBM Video/BBM Voice
- Non-Email Accounts
- Other Messaging Services
- PIN Messages
- SMS/MMS

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Controlling logging

By default, work space only devices don't synchronize log files for BlackBerry Messenger, Phone, SMS, MMS, PIN, and BBM Video chat features with the BlackBerry Device Service.

If you need to log one or more of these communication paths, you can use the following IT policy rules:

- BlackBerry Messenger Log Wireless Synchronization
- Phone Log Wireless Synchronization
- PIN to PIN Log Wireless Synchronization
- SMS/MMS Log Wireless Synchronization
- Video Chat Log Wireless Synchronization

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Controlling apps

By default, users can use certain apps developed by Research In Motion or installed by wireless service providers on work space only devices. You can use the following IT policy rules to make these apps unavailable on devices:

- BlackBerry Maps
- Wireless Service Provider Apps
- YouTube for BlackBerry Devices

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Related information

BlackBerry World for Work, 78
Controlling messaging, 77

BlackBerry World for Work

During work space only activation, the BlackBerry World for Work app is loaded on devices.

BlackBerry World for Work contains a Company Apps tab and a Public Apps tab that lists optional apps. The Company Apps tab provides a list of optional apps that are hosted by your organization. The Public Apps tab provides a list of apps from the public BlackBerry World app.

Users can only install apps that you deploy using the BlackBerry Device Service and public BlackBerry World apps that you specify as optional apps. Users can't install apps that haven't been approved by your organization.

If any of the apps that you specify as optional apps do not meet specific criteria for devices (for example, service provider, country, or device version), the apps won't appear in BlackBerry World for Work on those devices.

Devices classify Android apps as personal apps and personal apps can't be installed on work space only devices. If you specify an Android app from the public BlackBerry World as an optional app, it won't appear in BlackBerry World for Work on devices.

For more information about adding apps to BlackBerry World for Work, see the *BlackBerry Device Service Advanced Administration Guide*.

Related information

Managing app availability on devices, 83
Managing work apps using the BlackBerry World for Work storefront, 54

Controlling access

By default, users can provide other devices and apps with access to certain areas and information on their devices.

You can use the following IT policy rules to control what users can allow other devices and apps to have access to:

- Computer Access to Device
- Find More Contact Details
- Location Services
- Media Sharing

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Controlling features

You can use the following IT policy rules to control what users can do on their devices:

- Camera
- HDMI

- Roaming
- Voice dictation
- Voice control

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Controlling voice control

By default, users can use voice control commands on BlackBerry 10 devices. To prevent users from using voice control commands for Email and Calendar apps on devices, set the "Voice Control" IT policy rule to Disallow for Email and Calendar. To prevent users from using any voice commands on devices, set this rule to Disallow.

For more information, visit blackberry.com/go/kbhelp to read article KB33430.

Controlling software

By default, users can back up, restore, and update their device software.

Users can use BlackBerry Link to back up and restore apps and data on work space only devices. A user can restore data to a device after a device software update or if an issue occurs and the information needs to be restored. A user can restore data to the same device or transfer it to another device. Backed up data is encrypted and stored on the user's computer. To prevent users from backing up and restoring device data, set the "Backup and Restore Device" IT policy rule to Disallow. When you do this, the option to back up and restore data is disabled in BlackBerry Link.

Users can also update their device software by downloading BlackBerry 10 OS updates over the wireless network. Users can download all software updates that Research In Motion or a wireless service provider makes available. To limit users to downloading only security-related software updates over the wireless network that RIM or the wireless service provider makes available, you can set the "Wireless Software Updates" IT policy rule to Allow Security Updates Only. To prevent users from downloading any software updates over the wireless network, set the "Wireless Software Updates" to Disallow.

For more information about these IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

Related information

Back up and restore, 101

Controlling wallpaper

You can apply a customized wallpaper image to the home screen on work space only devices. After you specify an image file, the BlackBerry Device Service sends the wallpaper image to devices in the BlackBerry Enterprise Service 10 domain and users cannot change their wallpaper to a different wallpaper image.

If you don't send a work space wallpaper image to a device, users can set a wallpaper image using the Wallpaper option on devices. If users select images for wallpaper, devices save copies of the images in case they are deleted or the media cards that they are stored on are removed from devices.

Wallpaper images that you send to devices are stored in a protected folder on devices that is separate from the folders that store other wallpaper images and is removed if the devices are wiped.

For more information about sending wallpaper images to devices, see the *BlackBerry Device Service Advanced Administration Guide*.

Controlling app connections

The BlackBerry Device Service controls how apps on work space only devices connect to your organization's network. Because work space only devices are entirely controlled by your organization, all apps and data on these devices are considered work apps and work data. You can use IT policy rules to control the type of connections that work apps use to connect to your organization's network.

Work apps can access your organization's network using a number of communication methods. Based on the settings of IT policy rules, certain connections are available to apps on work space only devices. These connections are prioritized, and apps usually use the default route.

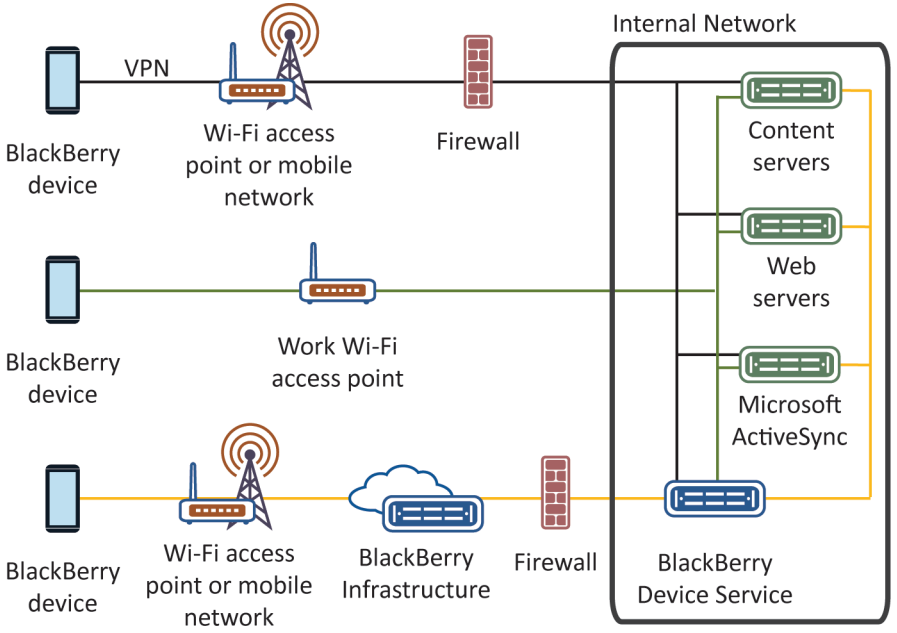
The "Network Access Control for Work Apps" and "Work Data Uses Only Work Network" IT policy rules control what connections are available to apps on work space only devices:

- The "Network Access Control for Work Apps" IT policy rule controls whether work apps on a device must connect to your organization's network through the BlackBerry Device Service.
- The "Work Data Uses Only Work Network" IT policy rule controls whether a device must route work traffic through a work VPN or work Wi-Fi connection and can't go through the BlackBerry Infrastructure.

If the "Network Access Control for Work Apps" IT policy rule is set to No, work apps attempt to connect to your organization's network using the following communication methods, in order:

1. Work VPN profiles over a Wi-Fi network
2. Work VPN profiles over a mobile network
3. Work Wi-Fi profiles
4. BlackBerry Infrastructure over a Wi-Fi network
5. BlackBerry Infrastructure over a mobile network

However, if the "Work Data Uses Only Work Network" IT policy rule is set to Yes, devices can't make any BlackBerry Infrastructure connections.

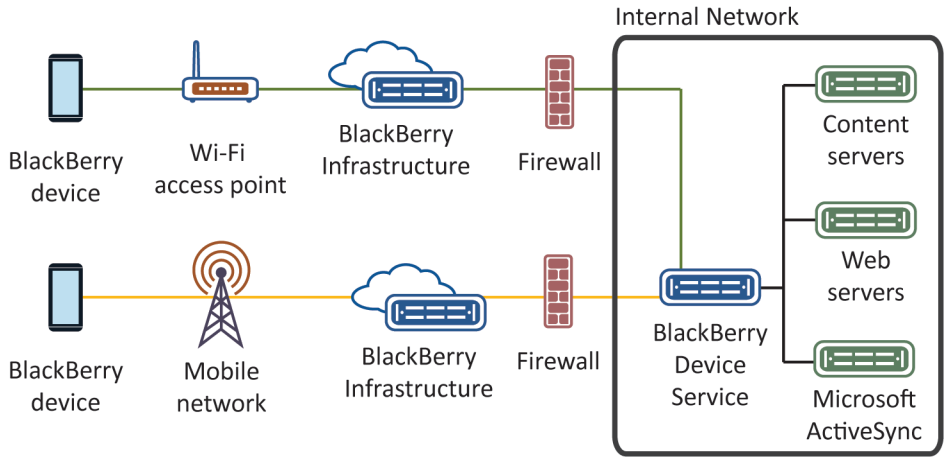


By default, work apps can use Wi-Fi profiles, VPN profiles, or the BlackBerry Device Service to connect to your organization's network. If you want to control or filter all work traffic on devices, you can set the "Network Access Control for Work Applications" IT policy rule to Yes. When you set this rule to Yes, you disable Wi-Fi and VPN connections for work apps and limit connectivity exclusively to the BlackBerry Device Service (using the BlackBerry MDS Connection Service and the BlackBerry Infrastructure).

If the "Network Access Control for Work Apps" IT policy rule is set to Yes, work apps attempt to connect to your organization's network using the following communication methods, in order:

1. BlackBerry Infrastructure over a Wi-Fi network
2. BlackBerry Infrastructure over a mobile network

In this case, also setting the "Work Data Uses Only Work Network" IT policy rule to Yes will not allow any communication methods and therefore it is not recommended that you set both of these rules to Yes.


Internal Network
BlackBerry device
Wi-Fi access point
BlackBerry Infrastructure
Firewall
Content servers
Web servers
BlackBerry device
Mobile network
BlackBerry Infrastructure
Firewall
BlackBerry Device Service
Microsoft ActiveSync

Managing app availability on devices

10

You can use the BlackBerry Device Service to install and manage work apps in the work space on devices. Work apps can only access work data and interact with other work apps.

A work app can be either an internal app or a public app available from the BlackBerry World storefront. You can add an internal app to the BlackBerry Device Service by specifying the .bar file using the BlackBerry Administration Service. The BlackBerry Device Service then adds the internal app to your organization's shared network folder.

You can specify the internal work apps that you want to install, update, or remove, and you can specify whether internal apps are required or optional on devices. You can also specify the BlackBerry device models that support an internal app so that the app is installed only on compatible devices. If you specify that an app is required, the app is automatically installed on the device and the user cannot remove it.

For BlackBerry 10 devices, you can also specify apps that are available to the public in BlackBerry World as optional work apps. If you specify a public app as an optional work app, the app becomes available to the user in the Public Apps tab of the BlackBerry World for Work storefront and the user can choose to install the app. Public apps that are specified as optional work apps cannot be required.

BlackBerry Balance devices (excluding BlackBerry PlayBook tablets) can have the same app installed separately in the work space and the personal space. Each instance of the app is kept separate from the other and each operates under the rules and restrictions that apply to the space that it is installed in. The apps can be configured, upgraded, or removed independently, and changes to one instance have no effect on the other instance. For example, an instant messaging app installed in the personal space might be restricted from adding work contacts, while the same instant messaging app installed in the work space does not have that restriction.

App developers can use various development tools to create, test, and package apps so that you can install them on the devices in your organization's environment. For more information about the development tools, visit www.blackberry.com/developers.

Note: The work space on devices does not support BlackBerry Runtime for Android apps.

Related information

Managing work apps using the BlackBerry World for Work storefront, 54
BlackBerry World for Work, 78
How work apps are installed on a BlackBerry PlayBook tablet, 72

Preventing users from installing apps using development tools

App developers can use development tools to test apps that they are developing by installing the apps on devices using a USB or Wi-Fi connection.

You can use the "Restrict Development Mode" IT policy rule to prevent users from using development tools to install apps on BlackBerry Balance devices. Users cannot use development tools to install apps on work space only devices.

When development mode is not available on a device, users can only download and install apps from the BlackBerry World storefront and the BlackBerry World for Work storefront, and you can also send apps to devices using the BlackBerry Administration Service.

Signing apps

Before you can make an app that is developed by your organization available to BlackBerry 10 devices on the BlackBerry World for Work storefront or to BlackBerry PlayBook tablets on the Work tab on the BlackBerry World storefront, Research In Motion requires that the RIM signing authority system digitally sign the app.

The RIM signing authority system uses public key cryptography to authorize and authenticate the application code.

The developer must visit https://www.blackberry.com/SignedKeys to register the app with the RIM signing authority system so that the app can use the signing tool that is included with the BlackBerry development tools. The signing tool permits an app to request, receive, and verify a digital signature from RIM. When a user starts the app, the BlackBerry 10 OS or the BlackBerry PlayBook OS verifies that the RIM signing authority signed the application files and that the application files have not changed since that app was installed.

For more information about code signing apps, see http://www.blackberry.com/developers.

Protecting a device from malicious apps

Apps are tested to make sure that they do not interfere with the core functionality of devices before they are approved by Research In Motion and made available on the BlackBerry World storefront. RIM can remove any apps from BlackBerry World that were identified as potentially malicious or do not follow the BlackBerry World Vendor Agreement.

Extending messaging security on BlackBerry 10 devices

11

You can extend messaging security for the BlackBerry Device Service solution and permit BlackBerry 10 device users to send and receive S/MIME-protected email messages. Digitally signing or encrypting messages adds another level of security to email messages that users send or receive from their devices. Users can digitally sign or encrypt messages if they use a work email account that supports S/MIME-protected messages on devices. When a device is activated on the BlackBerry Device Service, you can require the device to sign, encrypt, or sign and encrypt messages, using S/MIME encryption when sending email messages using a work email address.

Digital signatures are designed to help recipients verify the authenticity and integrity of messages that users send. When a user digitally signs a message with their private key, recipients use the sender's public key to verify that the message is from the sender and that the message has not changed.

Encryption is designed to keep messages confidential. When a user encrypts a message, the device uses the recipient's public key to encrypt the message. The recipient uses their private key to decrypt the message.

Devices support keys and certificates in the following file formats and file name extensions:

- PEM (.pem, .cer)
- DER (.der, .cer)
- PFX (.pfx, .p12)

If users don't have a smart card, users need to store their private keys and a certificate for each recipient that they want to send an encrypted email message to on their devices. Users can store a key and certificates by importing the files from a work email message. Users must use their work email accounts to send signed or encrypted email messages.

Related information

How the BlackBerry Device Service manages email messages, 21

Extending messaging security on BlackBerry 10 devices using S/MIME protection

You can extend messaging security for the BlackBerry Device Service and permit users to send S/MIME-protected email messages on BlackBerry 10 devices. Users do not have to install additional software on devices to support S/MIME protection. Users can configure S/MIME preferences on devices in the BlackBerry Hub settings, including choosing certificates and encoding methods. Users can manage certificates on their devices in the Security and Privacy section of the System Settings.

If devices do not have S/MIME support turned on, devices will not be able to send signed or encrypted email messages. To send encrypted email messages, a user must have the recipient's public key on their device. To read encrypted email messages, a user must have their private key on their device or on a smart card. If users do not have their private keys on their devices, the devices will not be able to read S/MIME-encrypted messages, and the devices will display the message, "Unable to decode the message because you do not have the corresponding private key".

To send digitally signed email messages, a user must have their private key on the device.

The BlackBerry Device Service uses email profiles to configure S/MIME settings on devices. You can configure the following S/MIME profile settings:

S/MIME profile setting	Description
S/MIME messages	You can specify whether S/MIME is enabled on a device. • Allowed: users can choose whether or not to enable S/MIME on the device. This is the default value. S/MIME is not enabled on the device and must be enabled by users. • Required: S/MIME is automatically enabled on the device and cannot be disabled by users • Disallowed: S/MIME is automatically disabled on the device and cannot be enabled by users
Digitally signed S/MIME messages	You can make digital signing of outgoing messages allowed, required, or disallowed: • Allowed: users can choose whether or not to digitally sign S/MIME messages (default value) • Required: users must send digitally signed messages • Disallowed: users cannot send digitally signed messages

S/MIME profile setting	Description
Encrypted S/MIME messages	You can make encryption of outgoing messages allowed, required, or disallowed: • Allowed: users can choose whether or not to encrypt messages (default value) • Required: users must encrypt messages • Disallowed: users cannot encrypt messages
Allowed content ciphers	You can choose any or all of the following encryption algorithms that a device can use to encrypt S/MIME-protected email messages: • AES (256-bit) • AES (192-bit) • AES (128-bit) • Triple DES • RC2

If you set any of the S/MIME settings to Required, you must make sure that users have their private key on their devices or smart cards to sign or decrypt messages.

The following table shows the dependencies between the S/MIME profile settings that you can configure on the BlackBerry Device Service and the S/MIME options that users can configure on devices. Depending on what these are set to, the options in the Encoding drop-down list on the device change. The device ignores the value for some settings if a higher priority setting (for example, the S/MIME Messages profile setting) conflicts with the value for that setting.

S/MIME Messages profile setting	Encrypted S/MIME Messages profile setting	Digitally Signed S/MIME Messages profile setting	S/MIME options on device	Encoding drop-down on device
Allowed	Allowed	Allowed	User can turn S/MIME on or off	• Plain text • S/MIME [Sign] • S/MIME [Encrypt] • S/MIME [Sign and Encrypt]
	Allowed	Required	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Encrypt] • S/MIME [Sign and Encrypt]

S/MIME Messages profile setting	Encrypted S/MIME Messages profile setting	Digitally Signed S/MIME Messages profile setting	S/MIME options on device	Encoding drop-down on device
	Allowed	Disallowed	User can turn S/MIME on or off	• Plain text • S/MIME [Sign]
	Required	Allowed	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Sign] • S/MIME [Sign and Encrypt]
	Required	Required	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Sign and Encrypt]
	Required	Disallowed	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Sign]
	Disallowed	Allowed	User can turn S/MIME on or off	• Plain text • S/MIME [Encrypt]
	Disallowed	Required	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Encrypt]
	Disallowed	Disallowed	User can turn S/MIME on or off (but cannot encrypt or sign messages because the necessary profiles are set to Disallowed)	Plain text
Required	Allowed	Allowed	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Sign] • S/MIME [Encrypt] • S/MIME [Sign and Encrypt]
	Allowed	Required	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Encrypt] • S/MIME [Sign and Encrypt]
	Allowed	Disallowed	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Sign]

S/MIME Messages profile setting	Encrypted S/MIME Messages profile setting	Digitally Signed S/MIME Messages profile setting	S/MIME options on device	Encoding drop-down on device
	Required	Allowed	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Sign] • S/MIME [Sign and Encrypt]
	Required	Required	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Sign and Encrypt]
	Required	Disallowed	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Sign]
	Disallowed	Allowed	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Encrypt]
	Disallowed	Required	S/MIME is on. User cannot turn S/MIME off.	S/MIME [Encrypt]
	Disallowed (This setting is ignored)	Disallowed (This setting is ignored)	S/MIME is on. User cannot turn S/MIME off.	• S/MIME [Sign] • S/MIME [Encrypt] • S/MIME [Sign and Encrypt]
Disallowed	This setting is ignored	This setting is ignored	S/MIME is off. User cannot turn S/MIME on.	Plain text

For more information about S/MIME profile setting descriptions, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

For information about managing S/MIME-related email profiles, see the *BlackBerry Device Service Advanced Administration Guide*.

S/MIME certificates and S/MIME private keys on BlackBerry 10 devices

BlackBerry 10 devices use public key cryptography with S/MIME certificates and S/MIME private keys to encrypt and decrypt email messages.

Item	Description
S/MIME public key	When a user sends an email message from a device, the device uses the S/MIME public key of the recipient to encrypt the message. When a user receives a signed email message on a device, the device uses the S/MIME public key of the sender to verify the message signature.
S/MIME private key	When a user sends a signed email message from a device, the device hashes the message using SHA-1, SHA-2, or MD5. The device then uses the S/MIME private key of the user to digitally sign the message hash. When a user receives an encrypted email message on a device, the device uses the private key of the user to decrypt the message. The private key can be stored on the device or a smart card.

S/MIME encryption algorithms that BlackBerry 10 devices use

When you or a user turns on S/MIME encryption on BlackBerry 10 devices, the value of the "Allowed content ciphers" profile setting specifies that a device can use any of the following encryption algorithms to encrypt messages: AES-256, AES-192, AES-128, RC2, or Triple DES. You can change the value of the "Allowed content ciphers" setting to use a subset of the encryption algorithms if your organization's security policies require it.

If a user wants to send an email message to a recipient that the user previously received an email message from, the device is designed to store the encryption algorithms that the recipient's email application can support, and use one of those encryption algorithms. By default, if the device cannot determine the encryption algorithms that the recipient's email application can support, the device encrypts the email message using Triple DES.

Data flow: Sending an email message from a BlackBerry 10 device using S/MIME encryption

1. A user sends an email message from a BlackBerry 10 device. The device performs the following actions:
   a Checks the BlackBerry device keystore for the S/MIME certificate of the recipient
   b Encrypts the email message with the S/MIME certificate of the recipient
   c If the device is connected to the BlackBerry Infrastructure, uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message

d Sends the encrypted message to the BlackBerry Device Service

2. If the device is connected to the BlackBerry Infrastructure, the BlackBerry Device Service decrypts the BlackBerry transport layer encryption.
3. The BlackBerry Device Service sends the S/MIME-encrypted message to the recipient.
4. The recipient decrypts the S/MIME-encrypted message using their S/MIME private key.

Using S/MIME with a smart card

Devices that run BlackBerry 10 OS version 10.1 support using S/MIME with a smart card and includes tools to import certificates onto the devices. To use S/MIME with a smart card, a user needs to bind the device with the smart card.

After the user binds the smart card to the device, the user can see the list of S/MIME certificates that are stored on the smart card and choose which ones to import into the certificate store on the device. The private keys remain on the smart card. To sign messages or decrypt them, the device must be bound to the smart card.

Related information

BlackBerry Smart Card Reader, 104

Protecting data

12

The BlackBerry Device Service and BlackBerry devices offer security features to protect user information, including:

- Passwords
- Security timeout
- Data wipe
- Back up and restore
- Encryption
- Home screen messages
- Smart cards with BlackBerry Smart Card Reader

Passwords

You can use password protection to protect your organization's data and user information on devices.

You can also lock a device remotely and change its password.

Device passwords

BlackBerry Balance devices, excluding BlackBerry PlayBook tablets, require users to set a work space password by default. If you don't want users to have to enter a password to access work content and resources in the work space, you can set the "Password Required for Work Space" IT policy rule to No.

BlackBerry PlayBook tablets do not require users to set a work space password by default. If you want users to have to enter a password to access work content and resources in the work space, you can set the "Password Required for Work Space" IT policy rule to Yes.

On BlackBerry Balance devices, you can enforce either a work space password or a password for the entire device as follows:

Rule settings	Result
• Password Required for Work Space = Yes • Apply Work Space Password to Full Device = No	The Work Password (in the BlackBerry Balance settings on the device) is used as the work space password and the IT

Rule settings	Result
	policy rules in the Password rule group apply to the work space password. Users have the option to use their work space password as their device password using the “Set as device password” option in the BlackBerry Balance settings, or the “Device password can be connected to the BlackBerry Balance Password" option in the Device Password settings on the device.
• Password Required for Work Space = Yes • Apply Work Space Password to Full Device = Yes	The work password is used as the password for the entire device and the IT policy rules in the Password rule group apply to the password for the entire device. When a user unlocks the device, the work space is unlocked at the same time. Users can choose to lock the work space manually when they are using the personal space on devices.

Work space only devices require users to set a work space password and this is not optional. Because there is only a work space on these devices, password enforcement and options apply to the entire device.

You can use the following IT policy rules in the Password rule group to enforce additional password requirements on devices:

- Maximum Password Age
- Maximum Password Attempts
- Maximum Password History
- Minimum Password Complexity
- Minimum Password Length

For more information about IT policy rules, see the *BlackBerry Device Service Policy and Profile Reference Guide*.

A user can configure device password settings using the Device Password option in the Security and Privacy settings on BlackBerry 10 devices or the Password option in the Security settings on BlackBerry PlayBook tablets. If a user turns on personal data encryption using the Encryption option on devices, the user must set a device password. Devices permit users to make password settings more restrictive, but never less restrictive, than the password rules that you specify.

Password changes

You can lock a device remotely and change its password. You can use the BlackBerry Device Service to send the “Specify new device password and lock device” IT administration command to a device if the device is lost or if a user forgets their password. When you send the command, devices do the following:

Device type	Conditions	Result
BlackBerry Balance (excluding BlackBerry PlayBook tablets)	• Device has a work space password • Device does not have a full device password	• The command creates a full device password • The work space password is not affected • The entire device locks and the new password is the device password
	• Device has a work space password • Device has a full device password • The passwords are different	• The command changes the full device password • The work space password is not affected • The entire device locks and the new password is the device password
	• Device has a work space password • You enforce the work space password as the full device password using the "Apply Work Space Password to Full Device" IT policy rule	• The command changes the work space password • The command changes the full device password • The entire device locks, both passwords are synchronized, and the new password is the password for the entire device
	• Device has a work space password • The user sets the work space password as the full device password using the "Use as my device password" option	• The command changes the full device password • The work space password is not affected • The entire device locks and the new password is the device password
BlackBerry PlayBook tablet	• Device has a work space password • Device does not have a full device password	• The command changes the work space password • The work space locks and the new password is the work space password
	• Device has a work space password • Device has a full device password • Both passwords are different	• The command changes the work space password • The full device password is not affected • The work space locks and the new password is the work space password

Device type	Conditions	Result
	• Device has a work space password • You enforce the work space password as the full device password using the "Apply Work Space Password to Full Device" IT policy rule	• The command changes the work space password • The command changes the full device password • The entire device locks, both passwords are synchronized, and the new password is the password for the entire device
	• Device has a work space password • The user enforces the work space password as the full device password using the "Use as my device password" option	• The command changes the work space password • The full device password is not affected • The work space locks and the new password is the work space password
Work space only	• These devices only have a device password and that password is mandatory	• The entire device locks and the new password is the password for the entire device

If the BlackBerry Device Service cannot connect to a device because the device is off or not connected to a network, the command is sent after the device connects to a network. You can communicate the new password to the user verbally when the user locates the device. When the user unlocks the device, the device prompts the user to accept or reject the new password.

You can also control how often a user must change their password by specifying the time that can elapse before a device password expires using the "Maximum Password Age" IT policy rule.

BlackBerry Balance device users can change the work space password in the BlackBerry Balance settings on the device. If the "Apply Work Space Password to Full Device" IT policy rule is set to No, a user can choose to use the same password for the entire device.

For more information about sending the “Specify new device password and lock device” IT administration command to a device, see the *BlackBerry Device Service Advanced Administration Guide*.

Data flow: When you change the work space password on a BlackBerry Balance device running BlackBerry 10 OS

1. You send the "Specify new device password and lock device" IT administration command to the device.
2. The device sends the encrypted intermediate key to the Enterprise Management Web Service.
3. The Enterprise Management Web Service uses the private key that is associated with the device to decrypt the intermediate key and sends the intermediate key back to the device.

The Enterprise Management Web Service stores a unique private key for each device that is activated on the Enterprise Management Web Service.

4. The device performs the following actions:
   - Uses the intermediate key to rederive the work master key and decrypts the work domain key
   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the device
   - Generates a new intermediate key
   - Uses the new intermediate key to generate a new work master key and uses it to encrypt the work domain key
   - Encrypts the new intermediate key using the public key that the Enterprise Management Web Service associates with the device and stores the encrypted key on the device

   Because only the Enterprise Management Web Service has the corresponding private key, only the Enterprise Management Web Service can decrypt the encrypted intermediate key. The intermediate key is never persistently stored on the device in unencrypted form.

   The work space password is reset.

Data flow: When a user changes the work space password on a BlackBerry Balance device running BlackBerry 10 OS

1. In the BlackBerry Balance settings on the device, the user types the current password and the new password.
2. The device authenticates the user by computing a SHA-512 hash of the current password and a stored 64-bit salt and compares the result with the stored hash of the current password.

   If the two hashes match, the work space unlocks and the password reset continues.
3. The device performs the following actions:
   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the device
   - Derives the current intermediate key
   - Uses the current intermediate key to derive the current work master key and decrypts the work domain key
   - Derives a new intermediate key
   - Uses the new intermediate key to derive a new work master key that it uses to encrypt the work domain key
   - Encrypts the new intermediate key using the public key that the Enterprise Management Web Service associates with the device and stores the encrypted key on the device

   Because only the Enterprise Management Web Service has the corresponding unique private key for each device that is activated on the Enterprise Management Web Service, only the Enterprise Management Web Service can decrypt the encrypted intermediate key. The intermediate key is not persistently stored on the device in unencrypted form.

   The work space password is reset.

Data flow: When you change the work space password on a BlackBerry PlayBook tablet

1. You send the "Specify new device password and lock device" IT administration command to the BlackBerry PlayBook tablet.
2. The tablet sends the encrypted intermediate key to the Enterprise Management Web Service.
3. The Enterprise Management Web Service uses the private key that is associated with the tablet to decrypt the intermediate key and sends the intermediate key back to the tablet.

   The Enterprise Management Web Service stores a unique private key for each tablet that is activated on the Enterprise Management Web Service.
4. The tablet performs the following actions:

   - Uses the intermediate key to rederive the work space key and decrypts the domain security record
   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the tablet
   - Generates a new intermediate key

     If the "Two-factor Encryption Key Generation" IT policy rule is set to Yes, the tablet uses the new password to generate the new intermediate key.

     If the "Two-factor Encryption Key Generation" IT policy rule is set to No, the tablet uses the domain key to generate the new intermediate key.
   - Uses the new intermediate key to generate a new work space key and uses it to encrypt the domain security record
   - Encrypts the new intermediate key using the public key that the Enterprise Management Web Service associates with the tablet and stores the encrypted key on the tablet

   Because only the Enterprise Management Web Service has the corresponding private key, only the Enterprise Management Web Service can decrypt the encrypted intermediate key. The intermediate key is never persistently stored on the tablet in unencrypted form.

   The work space password is reset.

Data flow: When a user changes the work space password on the BlackBerry PlayBook tablet

1. In the BlackBerry Balance settings on the BlackBerry PlayBook tablet, the user types the current password and the new password.
2. The tablet authenticates the user by computing a SHA-512 hash of the current password and a stored 64-bit salt and comparing the result with the stored hash of the current password.

   If the two hashes match, the work space unlocks and the password reset continues.
3. The tablet performs the following actions:

   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the tablet
   - Derives the current intermediate key

If the "Two-factor Encryption Key Generation" IT policy rule is set to Yes, the tablet uses the current password to derive the current intermediate key.

If the "Two-factor Encryption Key Generation" IT policy rule is set to No, the tablet retrieves and uses the domain key from the NV store to derive the current intermediate key.

- Uses the current intermediate key to derive the current work space key and decrypts the domain security record
- Derives a new intermediate key

  If the "Two-factor Encryption Key Generation" IT policy rule is set to Yes, the tablet uses the new password, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive the new intermediate key.

  If the "Two-factor Encryption Key Generation" IT policy rule is set to No, the tablet uses the domain key, a 128-bit random salt, and 20,000 iterations of the SHA-512 hash function to derive the new intermediate key.

- Uses the new intermediate key to derive a new work space key that it uses to encrypt the domain security record
- Encrypts the new intermediate key using the public key that the Enterprise Management Web Service associates with the tablet and stores the encrypted key on the tablet

Because only the Enterprise Management Web Service has the corresponding unique private key for each tablet that is activated on the Enterprise Management Web Service, only the Enterprise Management Web Service can decrypt the encrypted intermediate key. The intermediate key is not persistently stored on the tablet in unencrypted form.

The work space password is reset.

Security timeout

You can use the "Security Timeout" IT policy rule to require that a device lock the work space or the entire device after a certain period of inactivity.

On BlackBerry Balance devices, including BlackBerry PlayBook tablets, that have different work space and device passwords, the security timeout of the work space is controlled by the "Security Timeout" IT policy rule and the “Lock work space after” option (in the BlackBerry Balance settings on the device). The security timeout of the entire device is controlled by the “Lock Device After” option (in the Device Password settings on the device).

Work apps (including apps that display work data and personal data in a unified view) follow the security timeout for the work space, and if there is no user activity in the work space within the time specified, the work space locks automatically even if the user is using personal apps (not including apps that display work data and personal data in a unified view) at the time.

On BlackBerry Balance devices that have a work space password that applies to the full device, the security timeout of the entire device is controlled by the "Security Timeout" IT policy rule, along with the “Lock work space after” option (in the BlackBerry Balance settings on the device). The “Lock Device After” option (in the Device Password settings on the device) will be greyed out.

On work space only devices, because there is only a work space on these devices, the "Security Timeout" IT policy rule, along with the “Lock Device After” option (in the Device Password settings on the device), apply to the entire device. If there is no user activity on the device within the time specified, the entire device locks.

On BlackBerry 10 devices, certain apps, such as apps that display navigation information, slideshows, and videos, can extend the security timeout. By default, these apps can reset the security timer to prevent the device from locking after the period of user inactivity that you specify in the "Security Timeout" IT policy rule or specified in the Password Lock settings on the device. If you want to prevent apps from doing this, set the "Application Security Timer Reset" IT policy rule to Disallow. If the "Application Security Timer Reset" IT policy rule is set to Allow, users can still prevent apps from extending the password lock time in the Device Password settings on the device.

Data wipe

To protect your organization's data and user information on devices, you or a user can wipe data from devices as follows:

Device	What you can wipe
BlackBerry Balance device (including BlackBerry PlayBook tablet)	• Full device • Work space
Work space only device	• Full device

Full device wipe

Devices delete all data in the device memory, including all data on the media card when any of the following events occur:

Event	Device type	Description
You send the "Delete all device data and remove device" IT administration command to a device.	• BlackBerry Balance • Work space only	You can use the BlackBerry Device Service to send the "Delete all device data and remove device" IT administration command to the device to delete all data on the device. If the BlackBerry Device Service can't connect to the device because it is off or not connected to a network, the BlackBerry Device Service sends the command after the device connects to a network. For more information about sending this IT administration command, see the *BlackBerry Device Service Advanced Administration Guide*.
You send the "Delete only the organization data and remove device" IT administration command to a device.	• Work space only	You can use the BlackBerry Device Service to send the "Delete only the organization data and remove device" IT administration command to the device to delete all data on work space only devices. Because these devices only have a work space, you

Event	Device type	Description
		can use either the "Delete all device data and remove device" or "Delete only the organization data and remove device" IT administration commands to wipe these devices. If the BlackBerry Device Service can't connect to the device because it is off or not connected to a network, the BlackBerry Device Service sends the command after the device connects to a network. For more information about sending this IT administration command, see the *BlackBerry Device Service Advanced Administration Guide*.
A user types the device password incorrectly more times than the "Maximum Password Attempts" IT policy rule allows.	• BlackBerry Balance • Work space only	On BlackBerry Balance devices, when the device has one password for the entire device, if a user types the device password incorrectly more times than the "Maximum Password Attempts" IT policy rule allows, the device is wiped. On work space only devices, if a user types the device password incorrectly more times than the "Maximum Password Attempts" IT policy rule allows, the full device is wiped.
A user uses the Security Wipe option in the Security settings on the device.	• BlackBerry Balance • Work space only	A user can delete all data on devices using the Security Wipe option in the Security settings on the device.
A BlackBerry Balance device user uses BlackBerry Protect to delete all device data.	• BlackBerry Balance	On BlackBerry Balance devices, a user can also use BlackBerry Protect to wipe a device. For more information about BlackBerry Protect, see the *BlackBerry Protect User Guide*.

BlackBerry Balance devices, also delete all data from the work space when a full device wipe occurs.

Data flow: Deleting all data on the device

When you or a user deletes all data from a device, the device performs the following actions:

1. The BlackBerry 10 OS or BlackBerry PlayBook OS overwrites the device memory with zeros.
2. The BlackBerry 10 OS or BlackBerry PlayBook OS performs a secure TRIM operation on a section of device memory. The secure TRIM operation causes the flash memory chip to delete all of its memory.

Work space only wipe

To protect your organization's data on BlackBerry Balance devices, including BlackBerry PlayBook tablets, these devices delete all data in the work space when any of the following events occur:

Event	Description
You send the “Delete only the organization data and remove device” IT administration command to the device.	To require that a device delete all data in the work space, you can use the BlackBerry Device Service to send the “Delete only the organization data and remove device” IT administration command to the device. If the BlackBerry Device Service can’t connect to the device because it is off or not connected to a network, the BlackBerry Device Service sends the command after the device connects to a network. A user can still use the device while the work space data is being deleted. For more information about sending this IT administration command, see the *BlackBerry Device Service Advanced Administration Guide*.
The user types the work space password incorrectly more times than the "Maximum Password Attempts" IT policy rule allows.	When the device has a different work space and device passwords, if a user types the device password incorrectly more times than the "Maximum Password Attempts" IT policy rule allows, the work space is wiped.
The device exceeds the amount of time without connecting to your organization’s network that the "Wipe the Work Space Without Network Connectivity" IT policy rule allows.	You can use the "Wipe the Work Space without Network Connectivity" IT policy rule to specify the number of hours that must elapse when a device does not connect to your organization’s network before the device deletes all data in the work space. You can use this rule to make the device delete the data in the work space if the device can't receive updates or commands from the BlackBerry Device Service.
The user uses the "Delete work space" option in the BlackBerry Balance settings on the device.	Users can also remove the work space from their devices using the Delete option in the BlackBerry Balance settings.

When you or a user deletes all data from the work space on a device, the BlackBerry 10 OS or BlackBerry PlayBook OS instructs the file system to delete all directories and files in the work file system. Any files that persist in the work file system remain encrypted. The decryption keys are not accessible to the file system.

Back up and restore

Users can back up and restore apps and data on devices as follows:

Device	Spaces users can backup/restore	Software to use
BlackBerry Balance device (excluding BlackBerry PlayBook tablet)	• Work space • Personal space	• BlackBerry Link
Work space only device	• Work space	• BlackBerry Link
BlackBerry PlayBook tablet	• Personal space	• BlackBerry Link • BlackBerry Desktop Software

Backup protection

When a user backs up data and apps, the device encrypts the data and apps and then authenticates the backup file and header information before it sends the file to BlackBerry Link. BlackBerry Link then stores the file on the user's computer.

The device uses AES in CTR mode with a 256-bit key to encrypt and decrypt backup files and HMAC-SHA-256 to verify the integrity and authenticity of the backup files. Personal and work spaces are encrypted with different encryption keys.

To encrypt backup files for the personal space, the device uses a secret associated with the user's BlackBerry ID account to generate the encryption key and HMAC key. The secret is not accessible to the user and is never stored as part of the device backup file. The encryption key is stored on the device in an encrypted format.

To encrypt backup files for the work space, the devices uses a secret associated with the user's account associated with the BlackBerry Device Service to generate the encryption key and HMAC key. The secret is not accessible to the user and is never stored as part of the device backup file. The encryption key is stored in the device keystore in the work file system, which is encrypted.

The device uses the secret and a random salt to generate a 256-bit symmetric encryption key and a 256-bit authentication key. The device uses the encryption key to encrypt and decrypt the backup file and the authentication key to verify the integrity and authenticity of the backup file.

BlackBerry PlayBook tablet users can use BlackBerry Desktop Software to back up data instead of BlackBerry Link. If a tablet is running BlackBerry PlayBook OS 2.0.1 or later and a user selects Encrypt backup file in the File Options in the BlackBerry Desktop Software, the BlackBerry Desktop Software applies an additional layer of encryption to the backup file.

Restore protection

When a user restores backed up data and apps to a device, the device verifies the authenticity and integrity of the backup file before it decrypts and restores it.

To restore an encrypted backup file to the personal space on a new device during a device switch, the new device must use the same BlackBerry ID as the old device.

To restore an encrypted backup file to the work space on a new device during a device switch, the work space on the new device must be activated using the same user from your organization's user directory.

Encryption

Devices use encryption to protect the following:

- Work space data
- Personal space data
- Media card data

Work data

Devices protect work data by encrypting the files stored in the work space. Work space encryption is not optional.

Related information

How devices protect work data, 49
Work space encryption, 74
How BlackBerry PlayBook tablets protect work data, 64

Personal data

BlackBerry Balance devices can protect personal data by encrypting the files stored in the personal space.

Personal space encryption is optional. You can use the "Personal Space Data Encryption" IT policy rule to turn on encryption for the personal space on a device.

Users can also turn on personal data encryption using the Device Encryption option in the Security and Privacy settings on the device.

Related information

How devices protect personal data, 50
How a BlackBerry PlayBook tablet protects personal data, 67

Media cards

Devices can protect media card data by encrypting the files stored on media cards.

Media card encryption is optional. You can use the "Media Card Encryption" IT policy rule to turn on media card encryption.

Users can also turn on media card encryption using the Media Card Encryption option in the Security and Privacy settings on the device.

Related information

Protecting data on media cards, 50
Media card encryption, 74

Home screen message

If devices are lost, you can change the information that appears on the home screen to display contact information that can be used to return the device.

When you use the BlackBerry Device Service to send the "Specify new device password and lock device" IT administration command to a device, a message field appears. You can type the message that you want to appear on the home screen in the message field.

To change the home screen message, the device must be running BlackBerry 10 OS. For more information, see the *BlackBerry Device Service Advanced Administration Guide*.

BlackBerry Smart Card Reader

You can use the BlackBerry Smart Card Reader 2.0 with devices that run BlackBerry 10 OS version 10.1 to:

- Permit users to authenticate with their smart cards and log in (this is called two-factor authentication)
- Import the certificates that are required for S/MIME encryption

The reader communicates using Bluetooth technology version 1.1 and later and encrypts information on the smart card using AES-256 encryption. The reader stores all encryption keys in RAM only and never writes the keys to flash memory.

To pair devices with the reader, users must install a smart card driver, the BlackBerry Smart Card Reader driver, and, optionally, a smart card authenticator module on their devices.

Opening a secure connection to the BlackBerry Smart Card Reader

A user can open a secure connection between a BlackBerry 10 device and the BlackBerry Smart Card Reader in one of the following ways:

- Clicking Connect on the BlackBerry Smart Card Reader options screen on the device

- Trying an action on the device that requires the smart card (for example, importing certificates, signing or decrypting a message, or turning on two-factor authentication)

The reader reconnects automatically to a device that it has previously connected.

The device and reader open a secure connection by using the following pairings:

Pairing	Description
Bluetooth	This pairing creates a Bluetooth encryption key and opens a Bluetooth connection between the device and the reader. For more information about the Bluetooth connection, see the *BlackBerry Smart Card Reader Security Technical Overview*.
Secure pairing	This pairing creates a secure pairing PIN and opens a connection between the smart card and the device. The reader and the device use the secure pairing PIN to encrypt and authenticate the data that they send between them over the application layer. By default, the secure pairing PIN is 8 characters long and is case-sensitive. You can change the format of the secure pairing PIN using the "PIN Entry Mode" IT policy rule. During the secure pairing process the following events occur: • The initial key establishment protocol creates a shared device transport key on the device and the reader that they use to encrypt and decrypt the data that they send between them • The connection key establishment protocol creates a shared connection key on the device and the reader that they use to send data between them For more information about the initial key establishment protocol and the connection key establishment protocol, see the *BlackBerry Smart Card Reader Security Technical Overview*. The secure pairing is only deleted if the user removes the reader from the list of Bluetooth paired devices, or the device or reader is wiped.

Unbinding the current smart card from a device

There are two ways to delete the binding between a user's current smart card and a BlackBerry 10 device:

- You or a user wipes the device. During this process, the device deletes the smart card binding information from device memory. When the process completes, a user can authenticate with the device using a new smart card. You can wipe the device by sending the "Delete all device data and remove device" IT administration command or the "Delete only the organization data and remove device" IT administration command.
- The user turns off two-factor authentication. During this process, the device turns off two-factor authentication with the installed smart card and deletes the smart card binding information from the device.

Authenticating a user using a smart card

When you require a user to authenticate with a BlackBerry 10 device using a smart card, you turn on two factor authentication. Users need to prove their identities by demonstrating two factors:

- What they have (the smart card)
- What they know (their smart card password)

You can configure the "Two-Factor Authentication Only for Work Space" IT policy rule or "Assign Two-Factor Authentication for Work" IT policy rule to require that a user uses a smart card to authenticate when the user accesses the work space on a device. If you do not force the user to use a smart card to authenticate, the user can turn on or turn off two-factor authentication with the smart card by changing the User Authenticator field in the Security options on the device.

When you turn on two-factor authentication on the device, the following events occur:

1. The device pushes the current IT policy to the reader.
2. When a user tries to unlock the work space on the device, the device prompts the user to type the device password. If the user has not yet set a device password, the device forces the user to set a password.
3. The device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.
4. The device binds to the installed smart card automatically by encrypting and storing the smart card binding information in the base file system, which is designed to be inaccessible to the user.

When a user turns on two-factor authentication on the device, the following events occur:

1. The device prompts the user to type the device password. If the user has not yet configured a device password, the device forces the user to set a password.
2. The device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.

The BlackBerry 10 OS

13

The BlackBerry 10 OS is the microkernel operating system of the BlackBerry 10 device. Microkernel operating systems implement the minimum amount of software in the kernel and run other processes in the user space that is outside of the kernel.

Microkernel operating systems are designed to contain less code in the kernel than other operating systems. The reduced amount of code helps the kernel to avoid the vulnerabilities that are associated with complex code and to make verification easier. Verification is the process of evaluating a system for programming errors. Many of the processes that run in the kernel in a conventional operating system run in the user space of the BlackBerry 10 OS.

The BlackBerry 10 OS is tamper resistant. The kernel performs an integrity test when the BlackBerry 10 OS starts and if the integrity test detects damage to the kernel, the device does not start.

The BlackBerry 10 OS is resilient. The kernel isolates a process in its user space if it stops responding and to restart the process without negatively affecting other processes. In addition, the kernel uses adaptive partitioning to allocate resources to specific processes during overload conditions.

The BlackBerry 10 OS is secure. The kernel validates requests for resources and an authorization manager controls how apps access the capabilities of the device.

The BlackBerry 10 device file system

The BlackBerry 10 device file system runs outside of the kernel and keeps work data secure and, on BlackBerry Balance devices, separate from personal data. The BlackBerry 10 OS divides the file system into the following areas:

- Base file system
- Work file system
- Personal file system (on BlackBerry Balance devices)

The base file system is read-only and contains system files. Because the base file system read-only, the BlackBerry 10 OS can check the integrity of the base file system and mitigate the damage that an attacker who changes the file system can cause.

The work file system contains work data and apps. The device encrypts the files stored in the work space.

On BlackBerry Balance devices, the personal file system contains personal data and apps. Apps that a user installs on the device from the BlackBerry World storefront are located in the personal file system. The device can encrypt the files stored in the personal file system.

How the BlackBerry 10 OS uses sandboxing to protect app data

The BlackBerry 10 OS uses a security mechanism called sandboxing to separate and restrict the capabilities and permissions of apps that run on the BlackBerry 10 device. Each application process runs in its own sandbox, which is a virtual container that consists of the memory and the part of the file system that the application process has access to at a specific time.

Each sandbox is associated with both the app and the space that it is used in. For example, an app on a BlackBerry Balance device can have one sandbox in the personal space and another sandbox in the work space; each sandbox is isolated from the other sandbox.

The BlackBerry 10 OS evaluates the requests that an application's process makes for memory outside of its sandbox. If a process tries to access memory outside of its sandbox without approval from the BlackBerry 10 OS, the BlackBerry 10 OS ends the process, reclaims all of the memory that the process is using, and restarts the process without negatively affecting other processes.

When the BlackBerry 10 OS is installed, it assigns a unique group ID to each app. Two apps cannot share the same group ID, and the BlackBerry 10 OS does not reuse group IDs after apps are removed. An app's group ID remains the same when the app is upgraded.

By default, each app stores its data in its own sandbox. The BlackBerry 10 OS prevents apps from accessing file system locations that are not associated with the app's group ID.

An app can also store and access data in a shared directory, which is a sandbox that is available to any app that has access to it. When an app that wants to store or access files in the shared directory starts for the first time, the app prompts the user to allow access.

How the BlackBerry 10 OS manages the resources on a device

The BlackBerry 10 OS manages the BlackBerry 10 device resources so that an app cannot take resources from another app. The BlackBerry 10 OS uses adaptive partitioning to reallocate unused resources to apps during typical operating conditions and enhance the availability of the resources to specific apps during peak operating conditions.

How the BlackBerry 10 device manages permissions for apps

The authorization manager is the part of the BlackBerry 10 OS that evaluates requests from apps to access the capabilities of the BlackBerry 10 device. Capabilities include taking a photograph and recording audio. The BlackBerry 10 OS invokes the authorization manager when an app starts to set the permissions for the capabilities that the app uses. When an app starts, it might prompt the user to allow access to a capability. The authorization manager can store a permission that the user grants access to and apply the permission the next time that the app starts.

How the BlackBerry 10 device verifies the software that it runs

How the BlackBerry 10 device verifies the boot ROM code

The BlackBerry 10 device uses an authentication method that verifies that the boot ROM code is permitted to run on the device. The manufacturing process installs the boot ROM code in the processor on the device and the RIM signing authority system uses an RSA public key to sign the boot ROM code. The device stores information that it can use to verify the digital signature of the boot ROM code.

When a user turns on a device, the processor runs internal ROM code that reads the boot ROM from memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process completes, the boot ROM is permitted to run on the device. If the verification process cannot complete, the device stops running.

How the BlackBerry 10 device verifies the BlackBerry 10 OS and its file system

If the boot ROM code is permitted to run on the BlackBerry 10 device, the boot ROM code verifies the BlackBerry 10 OS. The BlackBerry 10 OS is digitally signed using EC 521 with a series of private keys. The boot ROM code uses the

corresponding public keys to verify that the digital signature is correct. If it is correct, the boot ROM code runs the BlackBerry 10 OS.

Before the BlackBerry 10 OS mounts the read-only base file system, it runs a validation program that generates a SHA-256 hash of the base file system content, including all metadata. The program compares the SHA-256 hash to a SHA-256 hash that is stored outside the base file system. This stored hash is digitally signed using EC 521 with a series of private keys. If the hashes match, the validation program uses the corresponding public keys to verify the signature and the integrity of the stored hash.

How the BlackBerry 10 device verifies apps and software upgrades

Once the base file system is validated, the BlackBerry 10 OS verifies existing apps by reading an app's XML file and verifying the assets of the app against the cryptographically signed hashes contained in the XML manifest.

Each software upgrade and app for the BlackBerry 10 device is packaged in the BlackBerry Archive (BAR) format. This format includes SHA-2 hashes of each archived file, and it includes an ECC signature that covers the list of hashes. When a user installs a software upgrade or app, the installation program verifies that the hashes and the digital signature are correct.

The digital signatures for a BAR file also indicate to the user the author of the software upgrade or app. The user can then decide whether to install the software based on its author.

Because the device can verify the integrity of a BAR file, the device can download BAR files over an HTTP connection, which makes the download process faster than over a more secure connection.

How the BlackBerry 10 device prevents the exploitation of memory corruption

The BlackBerry 10 device prevents exploitation of memory corruption in a number of different ways, including the six security mechanisms listed below.

Security mechanism	Description
Non-executable stack and heap	The stack and heap areas of memory are marked as non-executable. This means that a process cannot execute machine code in these areas of the memory, which makes it more difficult for an attacker to exploit potential buffer overflows.
Stack cookies	Stack cookies are a form of buffer overflow protection that helps prevent attackers from executing arbitrary code.

Security mechanism	Description
Robust heap implementations	The heap implementation includes a defense mechanism against the deliberate corruption of the heap area of memory. The mechanism is designed to detect or mitigate the overwriting of in-band heap data structures so that a program can fail in a secure manner. The mechanism helps prevent attackers from executing arbitrary code via heap corruption.
Address space layout randomization (ASLR)	By default, the memory positions of all areas of a program are randomly arranged in the address space of a process. This mechanism makes it more difficult for an attacker to perform an attack that involves predicting target addresses to execute arbitrary code.
Compiler-level source fortification	The compiler GCC uses the FORTIFY_SOURCE option to replace insecure code constructs where possible. For example, it might replace an unbounded memory copy with its bounded equivalent.
Guard pages	If a process attempts to access a memory page, the guard page raises a one-time exception and causes the process to fail. These guard pages are placed strategically between memory used for different purposes, such as the standard program heap and the object heap. This mechanism helps prevent an attacker from causing a heap buffer overflow and changing the behavior of a process or executing arbitrary code with the permissions of the compromised process.

The BlackBerry PlayBook OS

14

The BlackBerry PlayBook OS is the microkernel operating system of the BlackBerry PlayBook tablet. Microkernel operating systems implement the minimum amount of software in the kernel and run other processes in the user space that is outside of the kernel.

Microkernel operating systems are designed to contain less code in the kernel than other operating systems. The reduced amount of code helps the kernel to avoid the vulnerabilities that are associated with complex code and to make verification easier. Verification is the process of evaluating a system for programming errors. Many of the processes that run in the kernel in a conventional operating system run in the user space of the PlayBook OS.

The PlayBook OS is tamper resistant. The kernel performs an integrity test when the PlayBook OS starts and if the integrity test detects damage to the kernel, the tablet does not start.

The PlayBook OS is resilient. The kernel isolates a process in its user space if it stops responding and to restart the process without negatively affecting other processes. In addition, the kernel uses adaptive partitioning to allocate resources to specific processes during overload conditions.

The PlayBook OS is secure. The kernel validates requests for resources and an authorization manager controls how apps access the capabilities of the tablet.

The BlackBerry PlayBook tablet file system

The BlackBerry PlayBook tablet file system runs outside of the kernel and keeps work data secure and separate from personal data. The BlackBerry PlayBook OS divides the file system into the following areas:

- Base file system
- Personal file system
- Work file system

The base file system is read-only and contains system files. Because the base file system is read-only, the PlayBook OS can check the integrity of the base file system and mitigate the damage that an attacker who changes the file system can cause.

The personal file system contains the apps that run in personal mode and personal application data. Personal apps that a user installs on the tablet from the BlackBerry World storefront are located in the personal file system. The device can encrypt the files stored in the personal file system.

The work file system contains the apps that run in work mode and work application data. The tablet encrypts the work file system.

How the BlackBerry PlayBook OS uses sandboxing to protect app data

The BlackBerry PlayBook OS uses a security mechanism called sandboxing to separate and restrict the capabilities and permissions of apps that run on the BlackBerry PlayBook tablet. Each application process runs in its own sandbox, which is a virtual container that consists of the memory and the part of the file system that the application process has access to at a specific time.

Each sandbox is associated with both the app and the space that it is used in. For example, an app can have one sandbox in the personal space and another sandbox in the work space; each sandbox is isolated from the other sandbox.

The PlayBook OS evaluates the requests that an app's process makes for memory outside of its sandbox. If a process tries to access memory outside of its sandbox without approval from the PlayBook OS, the PlayBook OS ends the process, reclaims all of the memory that the process is using, and restarts the process without negatively affecting other processes.

When the PlayBook OS is installed, it assigns a unique group ID to each app. Two apps cannot share the same group ID, and the PlayBook OS does not reuse group IDs after apps are removed. An app's group ID remains the same when the app is upgraded.

By default, each app stores its data in its own sandbox. The PlayBook OS prevents apps from accessing file system locations that are not associated with the app's group ID.

An app can also store and access data in a shared directory, which is a sandbox that is available to any app that has access to it. When an app that wants to store or access files in the shared directory starts for the first time, the app prompts the user to allow access.

How the BlackBerry PlayBook OS manages the resources on a tablet

The BlackBerry PlayBook OS manages the tablet resources so that an app cannot take resources from another app. The PlayBook OS uses adaptive partitioning to reallocate unused resources to apps during typical operating conditions and enhance the availability of the resources to specific apps during peak operating conditions.

How the BlackBerry PlayBook tablet manages permissions for apps

The authorization manager is the part of the BlackBerry PlayBook OS that evaluates requests from apps to access the capabilities of the BlackBerry PlayBook tablet. Capabilities include taking a photograph and recording audio. The PlayBook OS invokes the authorization manager when an app starts to set the permissions for the capabilities that the app uses. When an app starts, it might prompt the user to allow access to a capability. The authorization manager can store a permission that the user grants access to and apply the permission the next time that the app starts.

How the BlackBerry PlayBook tablet verifies the software that it runs

How the BlackBerry PlayBook tablet verifies the boot ROM code

The BlackBerry PlayBook tablet uses an authentication method that verifies that the boot ROM code is permitted to run on the tablet. The manufacturing process installs the boot ROM code in the processor on the tablet and the RIM signing authority system uses an RSA public key to sign the boot ROM code. The tablet stores information that it can use to verify the digital signature of the boot ROM code.

When a user turns on a tablet, the processor runs internal ROM code that reads the boot ROM from memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process completes, the boot ROM is permitted to run on the tablet. If the verification process cannot complete, the tablet stops running.

How the BlackBerry PlayBook tablet verifies the BlackBerry PlayBook OS and its file system

If the boot ROM code is permitted to run on the BlackBerry PlayBook tablet, the boot ROM code verifies the BlackBerry PlayBook OS. The PlayBook OS is digitally signed using EC 521 with a series of private keys. The boot ROM code uses the

corresponding public keys to verify that the digital signature is correct. If it is correct, the boot ROM code runs the PlayBook OS.

Before the PlayBook OS mounts the read-only base file system, it runs a validation program that generates a SHA-256 hash of the base file system content, including all metadata. The program compares the SHA-256 hash to a SHA-256 hash that is stored outside the base file system. This stored hash is digitally signed using EC 521 with a series of private keys. If the hashes match, the validation program uses the corresponding public keys to verify the signature and the integrity of the stored hash.

How the BlackBerry PlayBook tablet verifies apps and software upgrades

Once the base file system is validated, the BlackBerry PlayBook OS verifies existing apps by reading an app's XML file and verifying the assets of the app against the cryptographically signed hashes contained in the XML manifest.

Each software upgrade and app for the BlackBerry PlayBook tablet is packaged in the BlackBerry Archive (BAR) format. This format includes SHA-2 hashes of each archived file, and it includes an ECC signature that covers the list of hashes. When a user installs a software upgrade or app, the installation program verifies that the hashes and the digital signature are correct.

The digital signatures for a BAR file also indicate to the user the author of the software upgrade or app. The user can then decide whether to install the software based on its author.

Because the tablet can verify the integrity of a BAR file, the tablet can download BAR files over an HTTP connection, which makes the download process faster than over a more secure connection.

How the BlackBerry PlayBook tablet prevents the exploitation of memory corruption

The BlackBerry PlayBook tablet prevents exploitation of memory corruption in a number of different ways, including the six security mechanisms listed below.

Security mechanism	Description
Non-executable stack and heap	The stack and heap areas of memory are marked as non-executable. This means that a process cannot execute machine code in these areas of the memory, which makes it more difficult for an attacker to exploit potential buffer overflows.

Security mechanism	Description
Stack cookies	Stack cookies are a form of buffer overflow protection that helps prevent attackers from executing arbitrary code.
Robust heap implementations	The heap implementation includes a defense mechanism against the deliberate corruption of the heap area of memory. The mechanism detects or mitigates the overwriting of in-band heap data structures so that a program can fail in a secure manner. The mechanism helps prevent attackers from executing arbitrary code via heap corruption.
Address space layout randomization (ASLR)	By default, the memory positions of all areas of a program are randomly arranged in the address space of a process. This mechanism makes it more difficult for an attacker to perform an attack that involves predicting target addresses to execute arbitrary code.
Compiler-level source fortification	The compiler GCC uses the FORTIFY_SOURCE option to replace insecure code constructs where possible. For example, it might replace an unbounded memory copy with its bounded equivalent.
Guard pages	If a process attempts to access a memory page, the guard page raises a one-time exception and causes the process to fail. These guard pages are placed strategically between memory used for different purposes, such as the standard program heap and the object heap. This mechanism helps prevent an attacker from causing a heap buffer overflow and changing the behavior of a process or executing arbitrary code with the permissions of the compromised process.

Protecting the data that the BlackBerry Device Service stores in your organization's environment

15

Data that the BlackBerry Configuration Database stores

The BlackBerry Configuration Database stores the following information:

- Name of the BlackBerry Device Service
- Unique SRP authentication keys and unique SRP IDs, or UIDs, that the BlackBerry Device Service uses in the SRP authentication process to open a connection to the BlackBerry Infrastructure
- IT policy private keys of the IT policy key pairs that the BlackBerry Device Service generates for each device
- Encryption keys that each device uses to encrypt and decrypt backup files
- Authentication keys that each device uses to authenticate backup files
- PIN of each device
- Read-only copies of each device transport key
- Copy of your organization’s user directory

Best practice: Protecting the data that the BlackBerry Configuration Database stores

Best practice	Description
Audit connections to the Microsoft SQL Server.	Consider the following guidelines: • At a minimum, write failed connection attempts to the Microsoft SQL Server log file and review the log file regularly. • When possible, save log files to a different hard disk drive than the one that the data files are stored on.
Delete unsecured, old setup files.	Consider deleting Microsoft SQL Server setup files that might contain plaintext, credentials encrypted with weak public keys, or sensitive information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during the Microsoft SQL Server installation process. Microsoft distributes the Killpwd tool, which is designed to locate and delete passwords from unsecured, old setup files in your organization's environment. For more information, visit www.support.microsoft.com to read article KB263968.
Limit the permission level of the Microsoft SQL Server.	Consider associating each Microsoft SQL Server service with a Windows account that the service derives its security context from. Microsoft SQL Server permits the sa account and, in some cases, other user accounts to access operating system calls based on the security context of the account that runs the Microsoft SQL Server service. If you do not limit the permission level of the Microsoft SQL Server, an attacker might use these operating system calls to attack any other resource that the account has access to.
Make the Microsoft SQL Server port numbers that are monitored by default on your organization's firewall unavailable.	Consider configuring your organization's firewall to filter packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.
Protect the sa account using a password.	Consider assigning a password to the sa account on the Microsoft SQL Server, even on servers that require Windows authentication. The password is designed to prevent an empty or weak password for the sa account from being exposed if an administrator of the database resets the Microsoft SQL Server for mixed mode authentication.

Best practice	Description
Protect the Microsoft SQL Server installation from Internet-based attacks.	Consider the following guidelines: • Require Windows Authentication Mode for connections to the Microsoft SQL Server to restrict connections to Windows user accounts and domain user accounts, and turn on credentials delegation. Windows Authentication Mode does not require you to store passwords on the computer. • Use stronger authentication protocols, required password complexity, and required expiration times.
Use a secure file system.	Consider the following guidelines: • Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and NTFS permits security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server specifies during the Microsoft SQL Server installation process. The Microsoft SQL Server creates appropriate ACLs on registry keys and files if it detects NTFS. • If you must change the account that runs the Microsoft SQL Server, decrypt the files that you could access using the old account and encrypt them again for access using the new account.
Use Microsoft SQL Server Management Studio.	Consider the following guidelines: • Use Microsoft SQL Server Management Studio to change the account that is associated with a Microsoft SQL Server service, if required. Microsoft SQL Server Management Studio configures the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account that is associated with a Microsoft SQL Server service. To use this applet, you must manually change the Windows registry, the permissions for the NTFS file system, and Windows user rights. For more information, visit www.support.microsoft.com to read article KB283811.

16 Cryptographic algorithms, codes, protocols, and libraries that devices support

BlackBerry devices support the following types of cryptographic algorithms, codes, protocols, and APIs:

- Symmetric encryption algorithms
- Asymmetric encryption algorithms
- Hash algorithms
- Message authentication codes
- Signature algorithms
- Key agreement algorithms
- Cryptographic protocols
- Cryptographic libraries
- VPN cryptographic support
- Wi-Fi cryptographic support

Symmetric encryption algorithms

Algorithm	Key length (in bits)	Modes
AES	128, 192, 256	CBC, CFB, ECB, OFB, CTR, CCM/CCM*, GCM, Key Wrap (RFC 3394)
AES	512	XTS
Blowfish	up to 256	CBC, CFB, ECB, OFB
Camellia	128, 192, 256	CBC, ECB
CAST	40 to 128	CBC, CFB, ECB, OFB

Algorithm	Key length (in bits)	Modes
DES	56	CBC, CFB, ECB, OFB
DESX	184	CBC, CFB, ECB, OFB
RC2	up to 256	CBC, CFB, ECB, OFB
RC4	up to 256	—
Triple DES	112, 168	CBC, CFB, ECB, OFB

Asymmetric encryption algorithms

Algorithm	Supported curve or key length (in bits)
ECIES	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
RSA PKCS#1 v1.5 / PKCS#1 v2.1 (OAEP)	512, 1024, 2048, 4096

Hash algorithms

Algorithm	Digest size (in bits)
AES-MMO	128
MD2	128
MD4	128
MD5	128
MDC-2	128
RIPEMD-160	160
SHA-1	160
SHA-2	224, 256, 384, 512

Message authentication codes

Codes	Key length (in bits)
AES-XCBC-MAC	128
CMAC-AES	28, 192, 256
HMAC-MD5	128
HMAC-SHA-1	160
HMAC-SHA-2	224, 256, 384, 512
HMAC-RIPEMD-160	160

Signature algorithms

Algorithm	Supported curve or key length (in bits)
DSA (FIPS 186-3)	1024, 2048, 3072
ECDSA	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
ECQV	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
RSA PKCS#1 v1.5 / PKCS#1 v2.1 (PSS)	512, 1024, 2048, 4096

Key agreement algorithms

Algorithm	Supported curve or key length (in bits)
DH	1024, 2048, 3072
ECDH	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
ECMQV	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1

Cryptographic protocols

Internet security protocols

- SSL 2.0
- SSL 3.0
- TLS 1.0

VPN security protocols

- IPSec
- IKE
- IKEv2

Wi-Fi security protocols

- WEP

- WPA-Personal
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise

Cipher suites that a device supports for opening SSL/TLS connections

A device supports various cipher suites for direct mode SSL/TLS when the device opens SSL/TLS connections to the BlackBerry Infrastructure or to web servers that are internal or external to your organization.

The device supports the following cipher suites when it opens SSL/TLS connections:

- TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_DSS_WITH_DES_CBC_SHA
- TLS_DHE_DSS_WITH_SEED_CBC_SHA
- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_SEED_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA

- TLS_ECDH_ECDSA_WITH_RC4_128_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_PSK_WITH_3DES_EDE_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_PSK_WITH_RC4_128_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_SEED_CBC_SHA

Cryptographic Libraries

- BlackBerry OS Cryptographic Library
- OpenSSL

VPN cryptographic support

Protocol	Authentication types	IKE IPSec DH group	IKE IPSec cipher	IKE IPSec hash	IKE PRF
IKE	PSK, PKI, XAUTH-PSK, XAUTH-PKI	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit keys)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
IKEv2	PSK, PKI, EAP-TLS, EAP-MS-CHAPv2	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit key)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

Wi-Fi cryptographic support

Cryptographic protocol	Encryption	EAP outer method	EAP inner method
WEP	RC4	—	—
WPA	TKIP	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS, EAP-AKA, EAP-SIM	MSCHAPv2, EAP-GTC, PAP

Cryptographic protocol	Encryption	EAP outer method	EAP inner method
WPA2	TKIP, CCMP (AES)	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS, EAP-AKA, EAP-SIM	MSCHAPv2, EAP-GTC, PAP

Product documentation

17

To read the following guides or additional related materials, visit blackberry.com/go/serverdocs.

Resource	Description
Introducing BlackBerry Enterprise Service 10	• Quick, visual introduction to BlackBerry Enterprise Service 10 at a high level
What's New in BlackBerry Enterprise Service 10 Quick Reference	• Summary of new features, enhancements, and updates in BlackBerry Enterprise Service 10
BlackBerry Enterprise Service 10 Product Overview	• Introduction to BlackBerry Enterprise Service 10 and its features • Finding your way through the documentation • Architecture
BlackBerry Enterprise Service 10 Release Notes	• Descriptions of known issues and potential workarounds
BlackBerry Enterprise Service 10 Installation Guide	• System requirements • Installation instructions
Capacity Calculator for BlackBerry Enterprise Service 10	• Tool to estimate the hardware required to support a given workload for BlackBerry Enterprise Service 10 version 10.1
BlackBerry Enterprise Service 10 Compatibility Matrix	• Software that is compatible with BlackBerry Enterprise Service 10 version 10.1
BlackBerry Enterprise Service 10 Upgrade Guide	• System requirements • Upgrade instructions
BlackBerry Enterprise Service 10 Licensing Guide	• Descriptions of different types of licenses • Instructions for activating licenses

Resource	Description
BlackBerry Enterprise Service 10 Configuration Guide	• Instructions for how to configure server components before you start administering users and their devices
BlackBerry Device Service Advanced Administration Guide	• Advanced administration for BlackBerry 10 devices and BlackBerry PlayBook tablets • Instructions for creating user accounts, groups, roles, and administrator accounts • Instructions for activating devices • Instructions for creating and sending IT policies and profiles • Instructions for managing apps on devices
Universal Device Service Advanced Administration Guide	• Advanced administration for iOS devices and Android devices • Instructions for creating user accounts, groups, and administrator accounts • Instructions for activating devices • Instructions for creating and sending IT policies and profiles • Instructions for managing apps on devices • Descriptions of IT policy rules for iOS devices and Android devices
BlackBerry Management Studio Basic Administration Guide	• Basic administration for all supported device types, including BlackBerry 10 devices, BlackBerry PlayBook tablets, iOS devices, Android devices, and BlackBerry 7.1 and earlier devices • Instructions for creating and managing user accounts in multiple Services • Instructions for managing multiple devices for each user account
BlackBerry Device Service Policy and Profile Reference Guide	• Descriptions of IT policy rules and profile settings for BlackBerry 10 devices and BlackBerry PlayBook tablets
BlackBerry Device Service Solution Security Technical Overview	• Description of the security maintained by the BlackBerry Device Service, BlackBerry Infrastructure, and BlackBerry 10 devices and BlackBerry PlayBook tablets to protect data and connections • Description of the BlackBerry 10 OS • Description of the BlackBerry PlayBook OS • Description of how work data is protected on BlackBerry 10 devices and BlackBerry PlayBook tablets when you use the BlackBerry Device Service

Resource	Description
BlackBerry Bridge App Security Technical Overview	• Description of how work data is protected on devices when you use the BlackBerry Bridge app • Description of how work data is protected when it is in transit between a BlackBerry PlayBook tablet and a BlackBerry smartphone • Description of attacks that the BlackBerry Bridge pairing process is designed to prevent

Glossary

18

A2DP	Advanced Audio Distribution Profile
ACL	An access control list (ACL) is a list of permissions that are associated with an object, such as a file, directory, or other network resource. It specifies which users or components have permission to perform specific operations on an object.
AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard Counter Mode CBCMAC Protocol
AES-XCBC	Advanced Encryption Standard extended cipher block chaining
AES-XCBC-MAC	Advanced Encryption Standard extended cipher block chaining message authentication code
API	application programming interface
ARC4	Alleged Rivest's Cipher 4
AVRCP	Audio/Video Remote Control Profile
BlackBerry Device Service solution	The BlackBerry Device Service solution consists of the BlackBerry Device Service and any components that connect to it such as messaging servers, databases, devices, a firewall, or the BlackBerry Infrastructure.
CA	certification authority
CAST	Carlisle Adams Stafford Tavares
CBC	cipher block chaining
CCKM	Cisco Centralized Key Management
CFB	cipher feedback
CKIP	Cisco Key Integrity Protocol
CSR	certificate signing request
CTR	Counter
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman
DoS	denial of service

DRBG	deterministic random bit generator
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol Authentication and Key Agreement
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol Generic Token Card
EAP-SIM	Extensible Authentication Protocol Subscriber Identity Module
EAPoL	Extensible Authentication Protocol over LAN
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
ECB	electronic code book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Standard
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
EDE	Encryption-Decryption-Encryption
EFS	Encrypting File System
FAT	File Allocation Table
FIPS	Federal Information Processing Standards
FQDN	fully qualified domain name
GCC	GNU Compiler Collection
GCM	Galois/Counter Mode
GPS	Global Positioning System
HFP	Hands-Free Profile
HMAC	keyed-hash message authentication code
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol over Secure Sockets Layer
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPPP	Internet Protocol Proxy Protocol
IPsec	Internet Protocol Security
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.
KDC	key distribution center
LAN	A local area network (LAN) is a computer network shared by a group of computers in a small area, such as an office building. Any computer in this network can communicate with another computer that is part of the same network.
LDAP	Lightweight Directory Access Protocol
MAP	Message Access Profile
MD	Message Digest Algorithm
MDC	Modification Detection Code
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging Service
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
NTLM	NT LAN Manager
NV	nonvolatile
NVRAM	nonvolatile random access memory
OBEX	Object Exchange

OFB	output feedback
OPP	Object Push Profile
PAC	Protected Access Credential
PAN	Personal Area Networking
PAP	Password Authentication Protocol
PBAP	Phone Book Access Profile
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PFX	Personal Information Exchange
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PRNG	pseudorandom number generator
PSK	pre-shared key
RACE	Research and Development in Advanced Communications Technologies in Europe
RC	Rivest's Cipher
RFC	Request for Comments
RIM signing authority system	The RIM signing authority system is used by third-party developers to cryptographically sign their applications.
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
S/MIME	Secure Multipurpose Internet Mail Extensions
SCEP	simple certificate enrollment protocol
SHA	Secure Hash Algorithm
SMS	Short Message Service
space	A space is a distinct area of the device that enables the segregation and management of different types of data, applications, and network connections. Different spaces can have different rules for data storage, application permissions, and network routing. Spaces were formerly known as perimeters.
SPN	A Service Principal Name (SPN) is an attribute of a user or group in Microsoft Active Directory that supports mutual authentication between a client of a Kerberos enabled service and the Kerberos enabled service. A Microsoft Active Directory account can have one or more SPNs.

SPP	Serial Port Profile
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP MD5	Transmission Control Protocol message digest algorithm 5
TGT	The Ticket Granting Ticket (TGT) is a service ticket that a client of a Kerberos enabled service sends to the TGS to request the service ticket for the Kerberos enabled service.
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
UID	unique identifier
URI	Uniform Resource Identifier
VPN	virtual private network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WTLS	Wireless Transport Layer Security
xAuth	Extended Authentication
XEX	Xor-Encrypt-Xor
XTS	XEX-based Tweaked CodeBook mode with CipherText Stealing

Legal notice

19

©2013 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Reader are trademarks of Adobe Systems Incorporated. Android is a trademark of Google Inc. Bluetooth is a trademark of Bluetooth SIG. Box is a trademark of Box, Inc. Documents To Go is a trademark of Dataviz, Inc. Dropbox is a trademark of Dropbox, Inc. Facebook is a trademark of Facebook, Inc. IEEE 802.11, IEEE 802.11i, and IEEE 802.1X are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Kerberos is a trademark of the Massachusetts Institute of Technology. Microsoft, Active Directory, ActiveSync, ActiveX, Internet Explorer, SQL Server, and Windows are trademarks of Microsoft Corporation. RSA is a trademark of RSA Security. Wi-Fi, WPA, WPA2, WPA-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise are trademarks of the Wi-Fi Alliance. YouTube is a trademark of Google Inc. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE

HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada